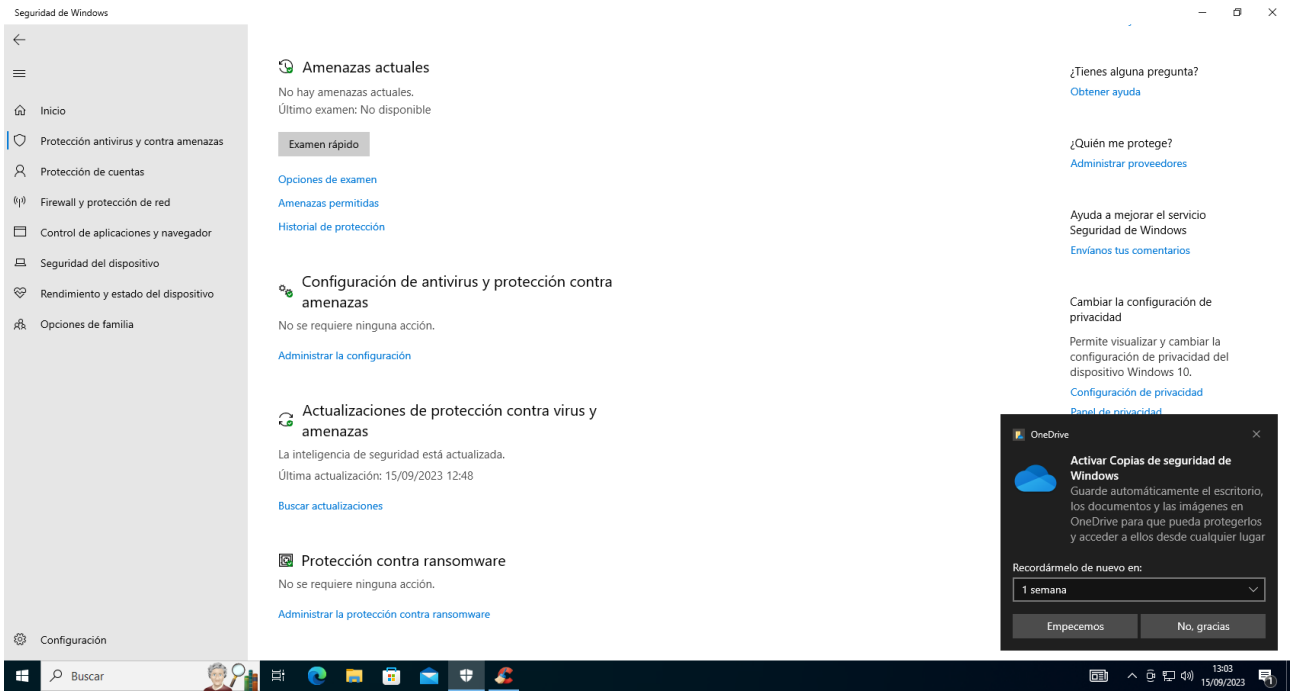
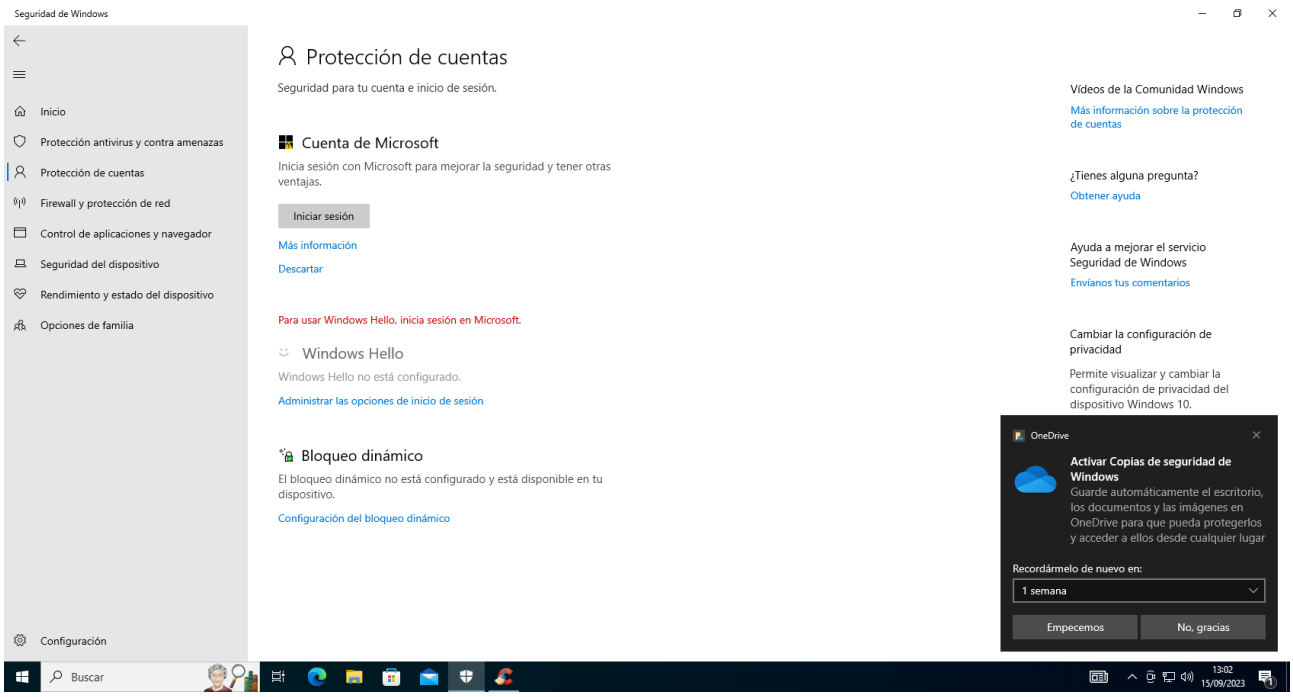
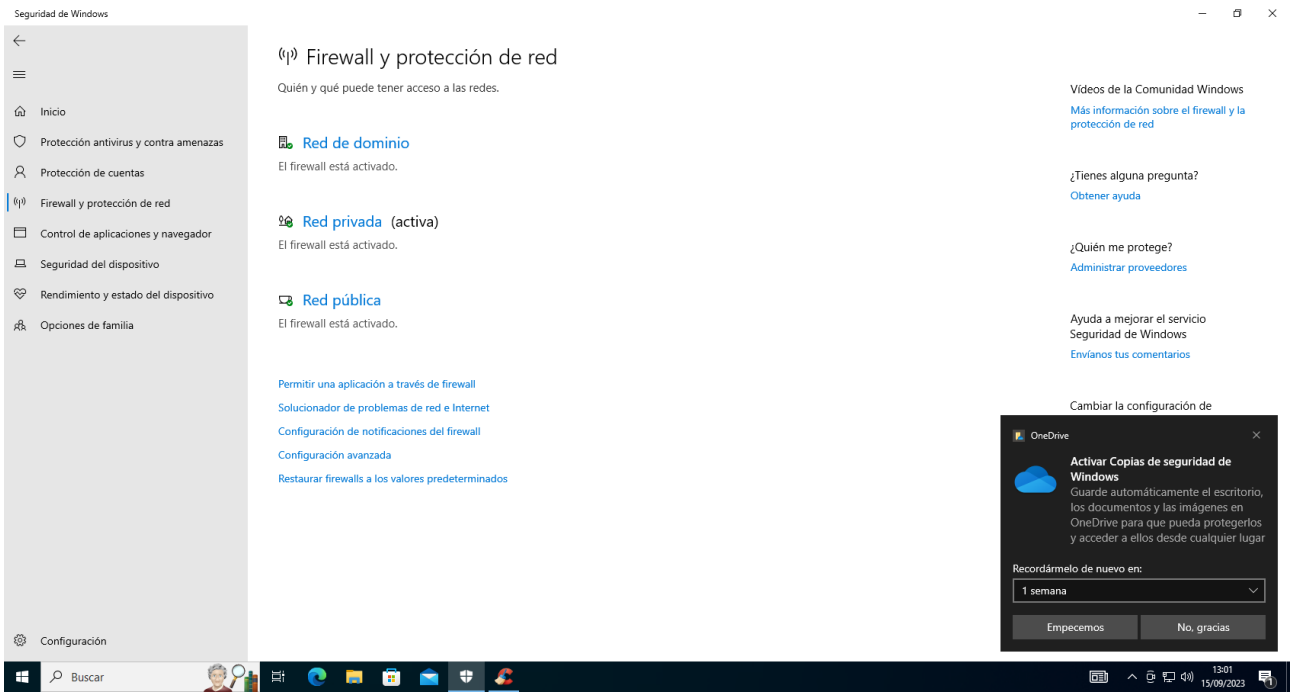
- ¿Qué es y para qué sirve el Windows Defender?
Windows Defender, ahora conocido como Microsoft Defender, es un programa de seguridad antivirus desarrollado por Microsoft. Su propósito es buscar y solucionar amenazas, prevenir, quitar y poner en cuarentena software espía y malware en Microsoft Windows. Es incluido y activado por defecto en Windows 8, Windows 8.1, Windows 10 y Windows 11.
- ¿Cuáles son sus funciones y todas sus características?
Las características básicas de Microsoft Defender son:
- Protección contra virus y amenazas: protección en tiempo real, protección contra virus y amenazas que se encuentran en el equipo, opciones de examen rápido, personalizado, completo y sin conexión. Protección basada en la nube, protección contra alteraciones y acceso controlado a carpetas.



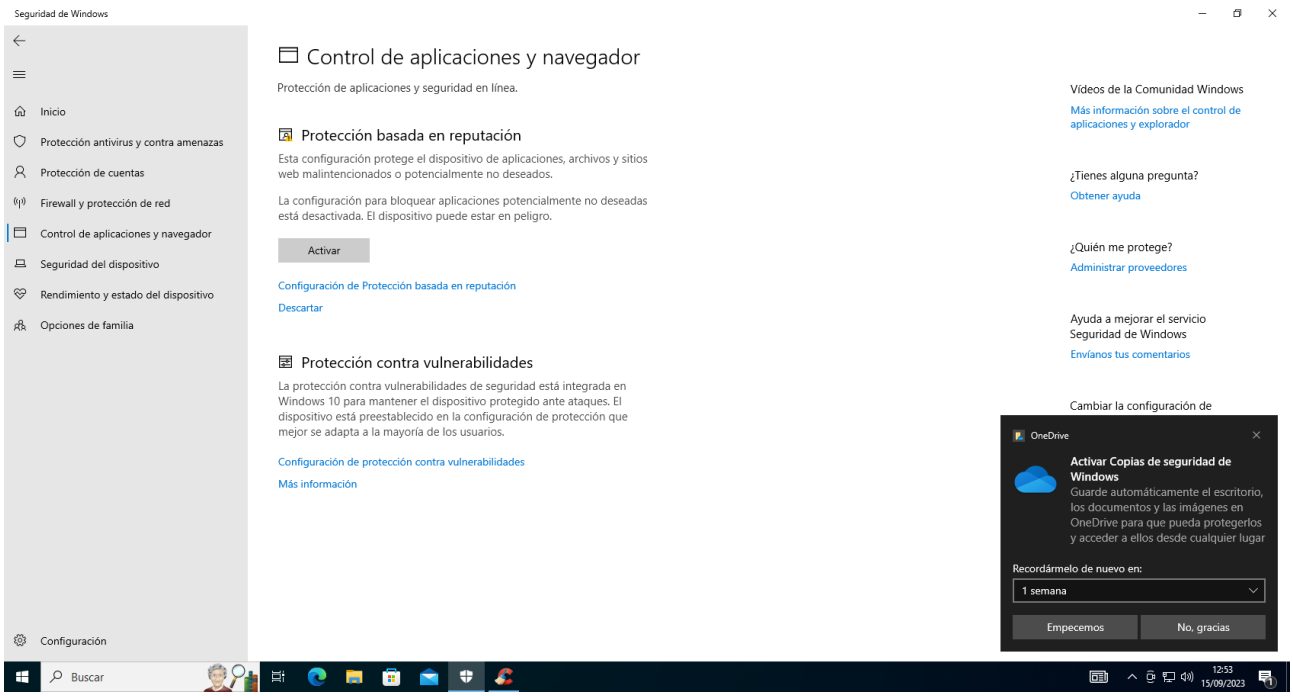
- Protección de cuentas: protege los inicios de sesión no autorizados y opciones de bloqueo dinámico por Bluetooth, esta opcion requiere cuenta de hotmail, esta pantalla es la siguiente:



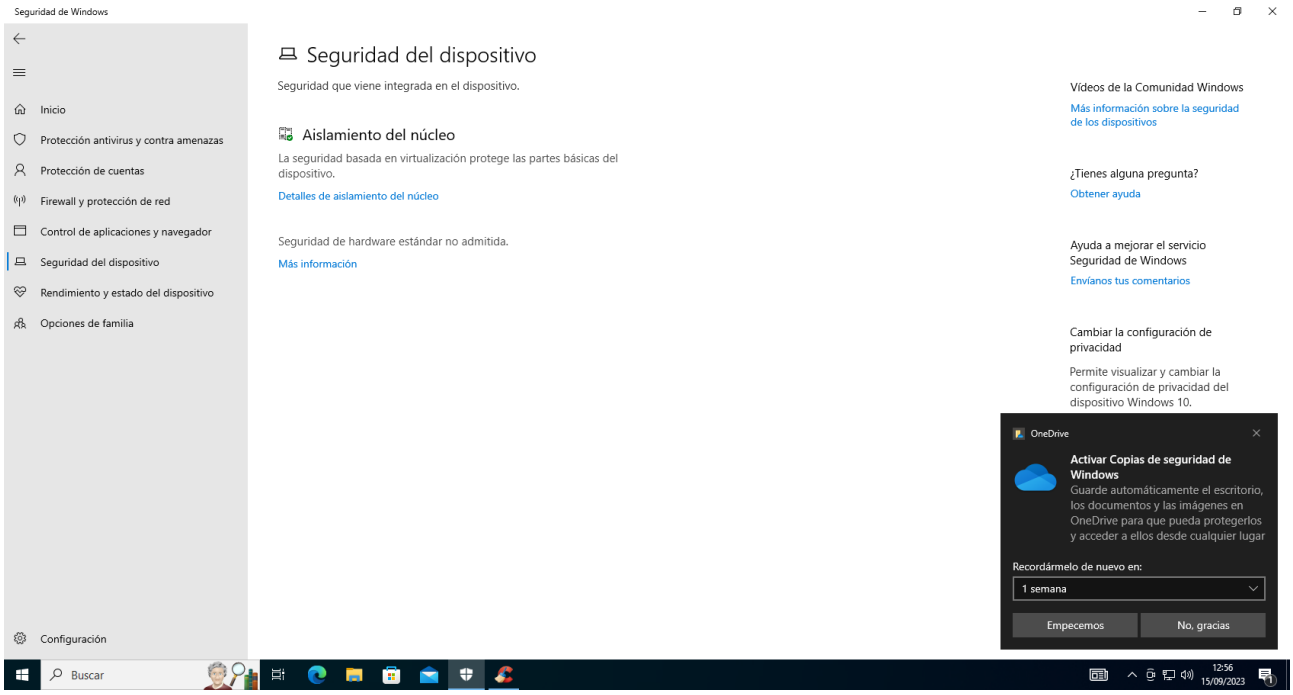
- Cortafuegos: protege al equipo de redes públicas, privadas y de dominio, permite elegir el tipo de red en la que te conectas para que el cortafuegos ofrezca una protección automática. Anteriormente, en XP, vista, 7 y 8-8.1 esta integrado en el sistema, pero no dentro del defender (en 8.1, solamente estaba dentro la parte del antivirus, en XP hasta el 7, hay que instalar el antivirus de microsoft manualmente [en windows update], que era el security essentials), las opciones que estan a partir de 10 son las siguientes:



- Control de aplicaciones y explorador: protege de programas, software o archivos potencialmente no deseados basado en la reputación para el navegador Edge, además ofrece opciones para proteger el equipo de vulnerabilidades.



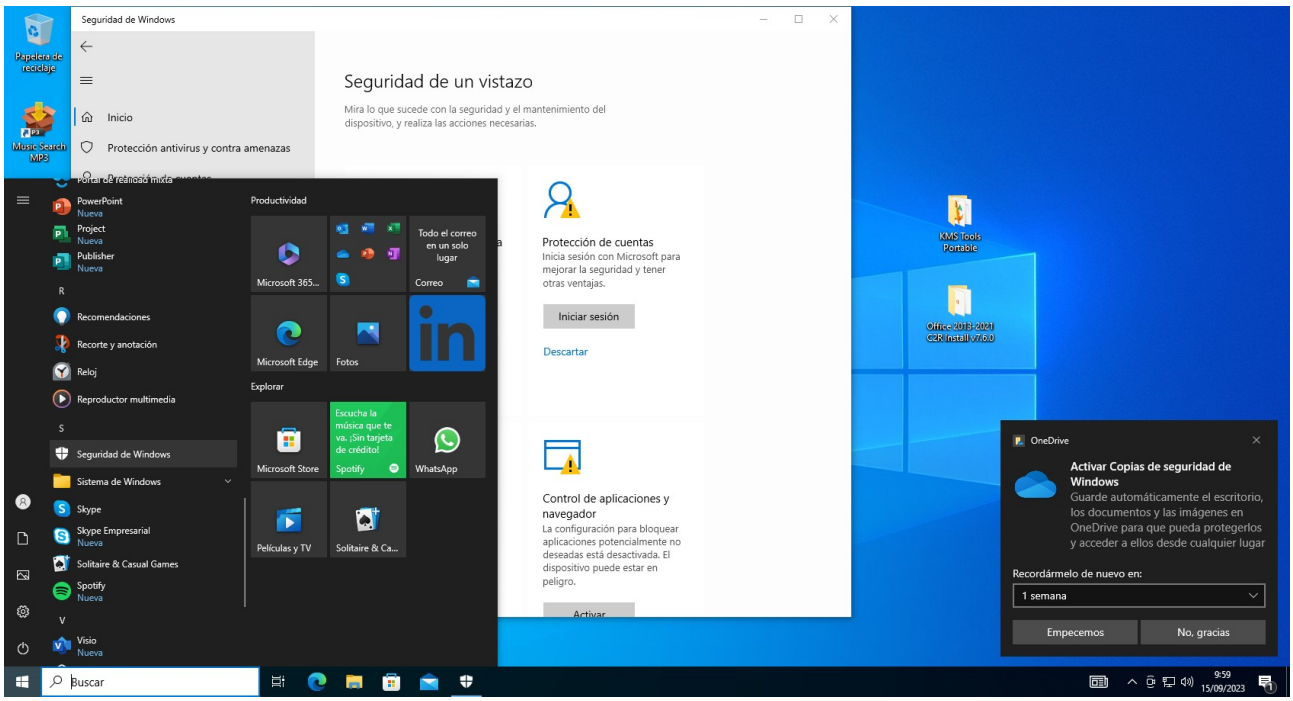
- Seguridad de hardware: Protección y aislamiento del núcleo basado en la virtualización.



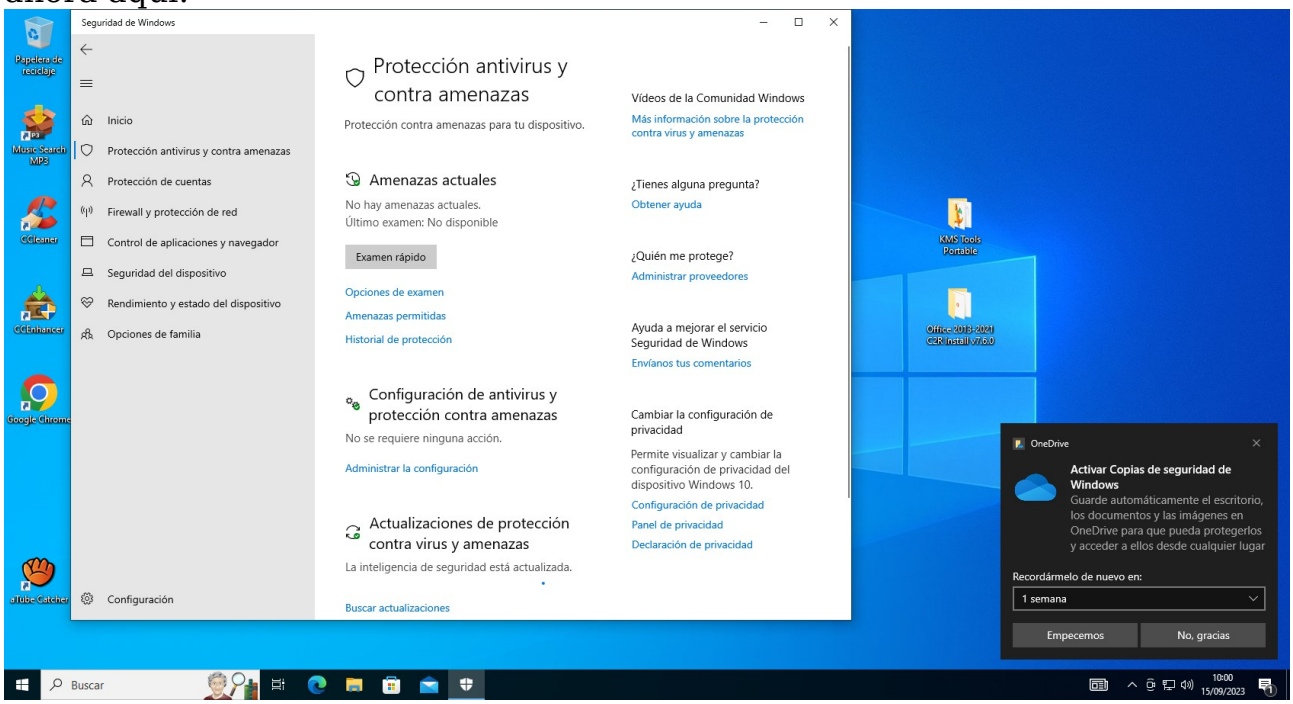
- ¿Qué opciones de detección tiene?
Para esta pregunta se dira la historia del defender a partir de windows 8.1, la idea de que microsoft creara un antivirus vino a partir de windows XP, con una solucion ya sustituida llamada microsoft security essentials, este antivirus se tenia que instalar manualmente via windows update (el metodo oficial ya ha sido eliminado por microsoft, aunque puede instalarse por metodos no oficiales como windows update restored o legacy update), por aquellos entonces el firewall no iba integrado en el antivirus, las opciones son las siguientes:

<u>windows 10</u>

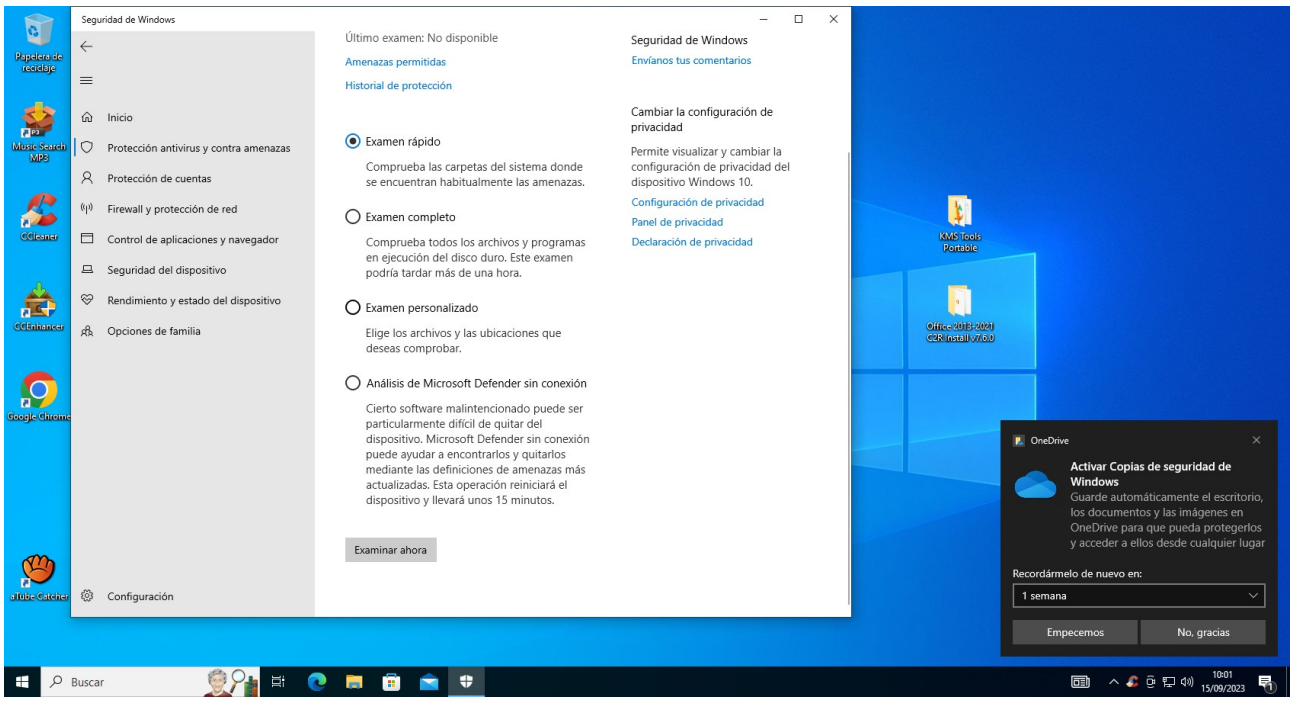
para windows 10 se va a inicio-seguridad de windows:



ahora aquí:



se le da a “opciones de examen” y aquí:



hay cuatro opciones, examen rapido, escanea solo el directorio del sistema, completo, lo escanea todo, personalizado, escanea lo que deseemos y analisis sin conexión, lo ejecuta desde un entorno limpio, este entorno, al reiniciarse el equipo se inicia una sesion en comandos donde te dice el porcentaje completado, cuando termine se reinicia automaticamente

windows 11

NOTA: windows 11 ya no se puede instalar en equipos intel por debajo de la octava generacion, en equipos intel xeon (para empresas) unicamente se puede instalar en equipos de la novena generacion, la noticia de la eliminacion de soporte del intel xeon de la octava generacion se puede consultar aquí:
https://hardzone.es/noticias/procesadores/intel-xeon-compatibles-windows-11/
https://www.muycomputer.com/2023/08/08/cambios-en-los-requisitos-de-windows-11-estos-procesadores-ya-no-son-compatibles/
los requisitos especiales que pide windows 11 son los siguientes:

- la BIOS tiene que ser la nueva (UEFI).
- La BIOS tiene que tener el secure boot.
- La placa tiene que tener TPM, que puede ir o por hardware (en las primeras placas, según he leido, el TPM se tenia que instalar manualmente, ahora el TPM va integrado a la placa) o por software (escrito en la BIOS), ademas tiene que ser el 2.0 (en los intel core I antiguos tiene una especificacion antigua de TPM)
- que el procesador figure en la lista oficial:

https://learn.microsoft.com/es-es/windows-hardware/design/minimum/supported/windows-11-supported-intel-processors

ademas de eso y si el equipo es de octava generacion, es posible que secure boot o TPM no esten integrados, para ello sera necesario actualizar la BIOS para que el 11 se pueda instalar sin problemas, ademas como se ha dicho, existen algunos modelos de placas base en los cuales hay que instalar el TPM manualmente (hay que mirar el manual de la placa, normalmente tiene un soporte especial en donde hay que instalar dicho modulo [que se vende por separado]), las actuales ya vienen soldadas a la placa, en el caso de que no

tenga TPM ni secure boot o unicamente tenga uno de los dos la placa, hay que actualizar la BIOS para poder instalar windows 11.

Este sistema se puede instalar en real en equipos no compatibles haciendo cambios en el registro, sin embargo, las utilidades rufus (para windows) y la utilidad para hacer pendrives multiboot ventoy ya pueden ajustar el registro de manera automatica para instalar el 11 en este tipo de equipos.

Al instalar en un equipo que no cumple los requisitos, saldra primero el siguiente aviso de microsoft:

Este equipo no cumple con los requisitos mínimos del sistema para ejecutar Windows 11: estos requisitos ayudan a garantizar una experiencia de confianza y de mayor calidad. No se recomienda instalar Windows 11 en este equipo ya que puede provocar problemas de compatibilidad. Si se procede a instalar Windows 11, el equipo ya no será compatible y no se podrán recibir actualizaciones. Si se producen daños en el equipo por falta de compatibilidad, no lo cubrirá la garantía del fabricante.

Ademas de eso saldran dos marcas de agua, primero el de los requisitos minimos y luego el clasico de la licencia.

Aunque el sistema se pueda instalar en equipos no compatibles, la experiencia no seria la misma, ya que podria provocar desde lentitud hasta pantallazos azules de la muerte por hardware incompatible, si se experimenta algun problema sera necesario volver a 10[1] o usar un sistema operativo libre como linux (se puede instalar por medio del arranque dual con windows) e instalar el entorno wine para arrancar los programas de microsoft con linux, esta solucion esta disponible para MAC OS y para linux (en windows no esta disponible), para las instrucciones con MAC (tanto arquitectura intel como apple), consultar el siguiente link:

https://wiki.winehq.org/MacOS

para linux, ir a la pagina del listado en donde dice las distros compatibles: https://wiki.winehq.org/Download

bien, si se quiere cargar el 11 en un equipo no compatible, se recomienda maquina virtual (que es lo que he hecho y donde se van a decir los pasos), en este caso, los requisitos son:

---

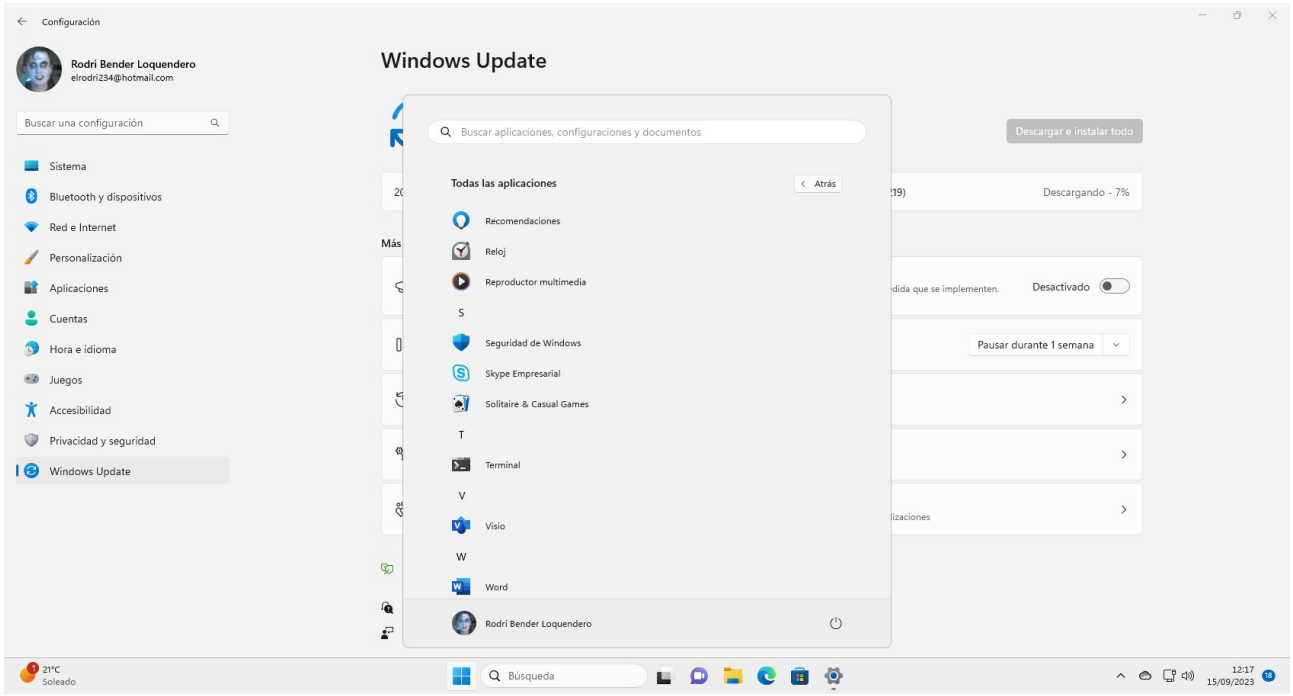
1 Este sistema caduca el 14 de octubre de 2025, según la hoja de la directiva del ciclo de vida de microsoft que se puede consultar aquí: https://learn.microsoft.com/es-es/lifecycle/
una vez ya caducado, microsoft ya no ofrecera soporte para clientes que tengan el 10 (antes de que microsoft emitiera licencias) ni tampoco ofrecera actualizaciones ni correcciones de seguridad, el sistema se puede seguir usando despues de esa fecha, pero solamente se recomienda hacerlo en maquina virtual, ademas de eso, es posible que algunos desarrolladores de hardware y de software “den la espalda” a windows 10 una vez ya alcanzado el fin de soporte, el usuario se tendria que enfrentar a las pantallas de los programas que digan “esta version del sistema ya no esta soportada para este programa, por favor actualice”

- el equipo tiene que ser I3-I5-I7, core 2 duo no vale (la memoria maxima que se le puede poner a las placas base con procesador intel core 2 duo son de 4 GB)
- actualizar los programas de virtualizacion a sus ultimas versiones (las ultimas versiones ya tienen un TPM “artificial” para que el 11 pueda ser virtualizado)
- el equipo real tiene que tener 8 GB o mas (requisito importante)
- el disco principal tiene que ser SSD, el segundo disco puede ser mecanico perfectamente (mi ordenador tiene un SSD de 1 TB y un mecanico de 4 TB), ya que lo que se va a hacer es que tire del archivo de paginacion (swap en linux).
- El equipo tiene que estar instalado en UEFI (he probado en “Modo normal” [legacy] y va lenta la maquina).
- El sistema operativo windows tiene que ser un modificado que quite los procesos innecesarios, si se tiene que poner tanta memoria RAM a un equipo virtual, se recomienda linux para que tanto en real como en virtual te vayan bien (ya que windows no destaca en tema procesos ni en apariencia, es decir, consume mas recursos que linux por sus procesos innecesarios y por la apariencia visual del sistema).
- El sistema tiene que tener configurado el archivo de paginacion a 16 GB para tener una experiencia mas o menos optima para la maquina virtual de 11.
- Prestar atencion a las pantallas de configuracion de la maquina, asegurarse que secure boot esta activado en la maquina virtual y que tenga la cantidad de memoria minima reservada en la maquina virtual.
- El secure boot (que en equipos atom y core I3-I5-I7 antiguos esta en algunas BIOS) si el equipo es no actualizable a 11 estorba, ya que lo que hace es controlar la ejecucion de software no firmado, ademas si se quiere migrar a linux (aconsejable para cargar el 11 en virtual, en pruebas hechas con server 2012 R2 con 4 GB a mi se me colgo windows al arrancar chrome y spotify [que lo uso mucho] con esa maquina arrancada) se recomienda tenerla desactivada, ya que las claves del secure boot cambian cada cierto tiempo y cuando cambian, podria no arrancar el linux (se puede restaurar desde cualquier linux entrando desde el modo recovery, en debian-ubuntu [boton ESC], darle a “network” para activar la red, luego a console y teclear apt-get update y apt-get dist-upgrade para instalar las nuevas claves del secure boot)
- la caracteristica intel VT/X (lectura de maquinas virtuales de 64 bits), tiene que estar activada en la BIOS.

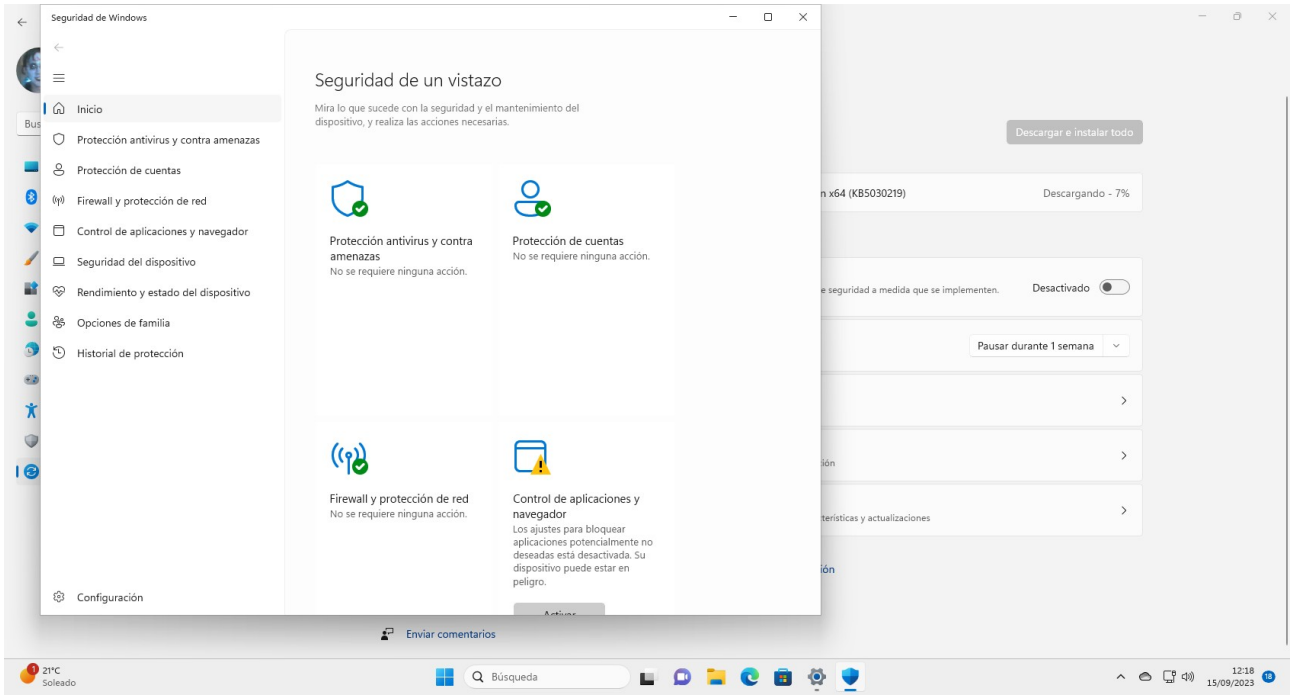
Bien, con esta configuración, se podra instalar 11 en entornos virtualizados sin que salten los errores establecidos por microsoft, si se instala el sistema en equipos no compatibles

bien, una vez ya dicho todo, vamos a ver las opciones de escaneo que estan en el defender de 11:

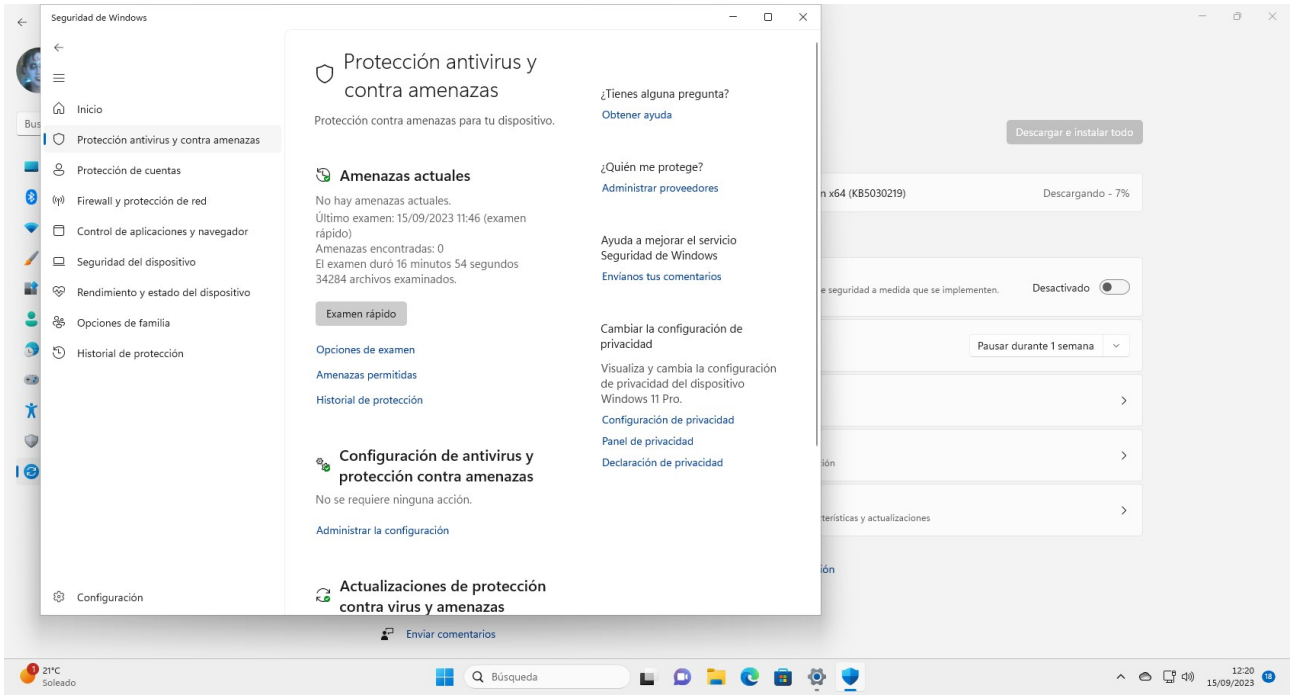
bien, el acceso es en inicio-todas las aplicaciones-seguridad de windows:



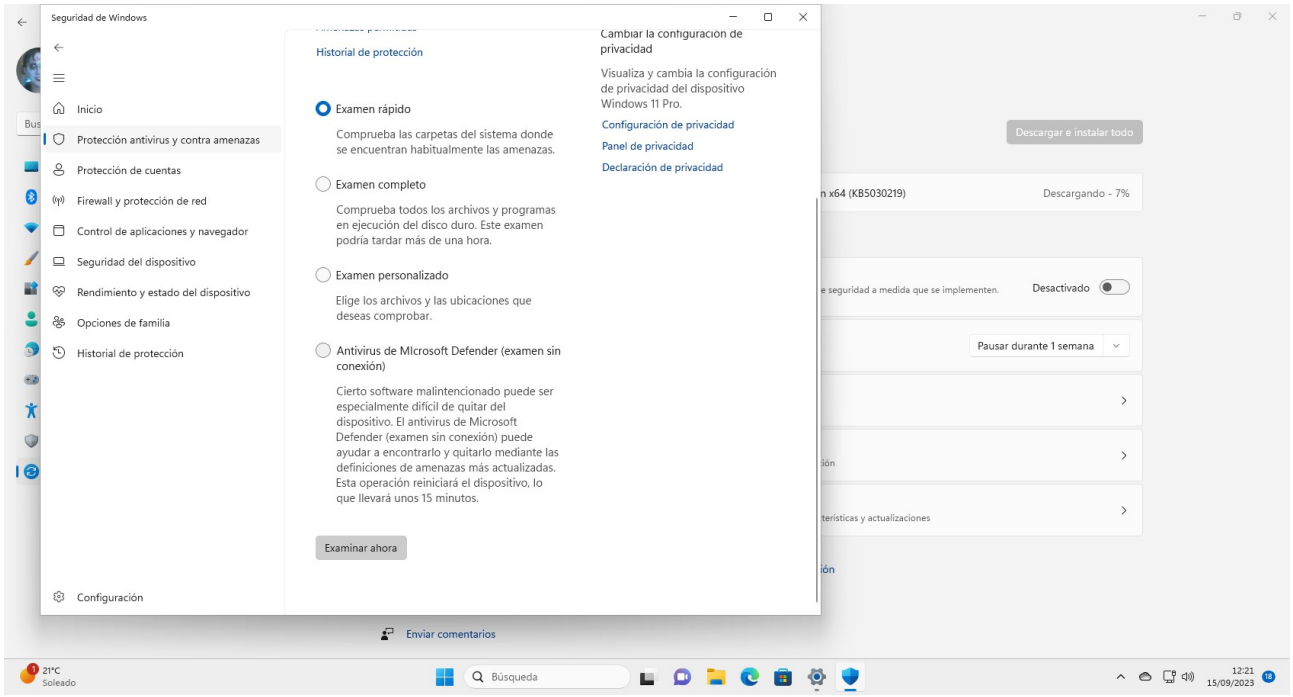
bien, aquí:



damos en “protección antivirus” y aquí:



darle a “opciones de examen”, a partir de aquí:

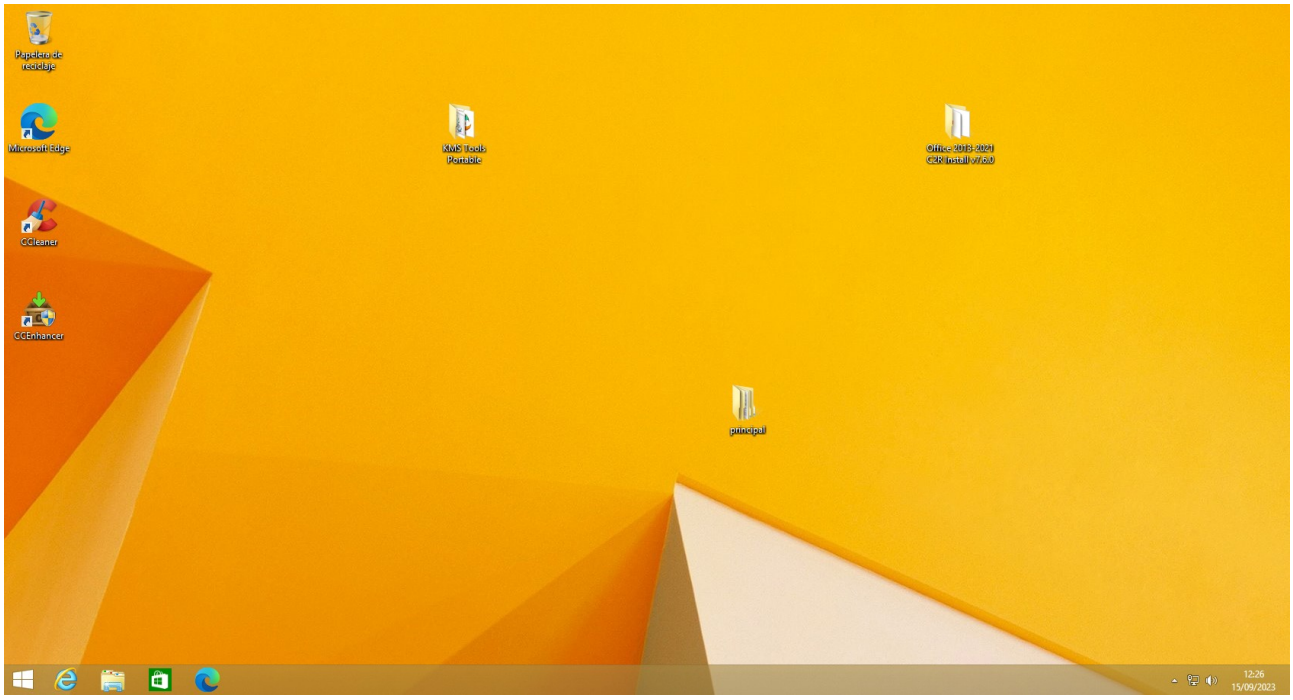


misma pantalla que en 10.

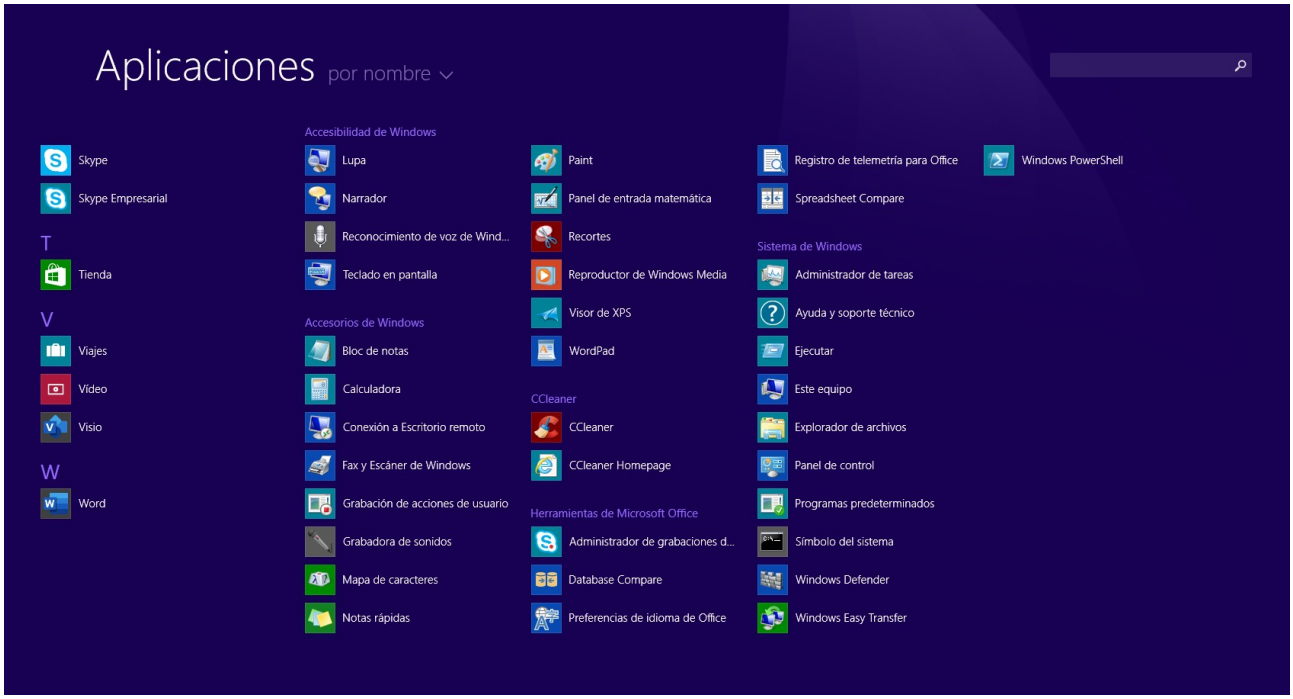
windows 8.1

este sistema (que solo ha sido prorrogado para su variante server), la pantalla cambia radicalmente, los pasos son los siguientes:

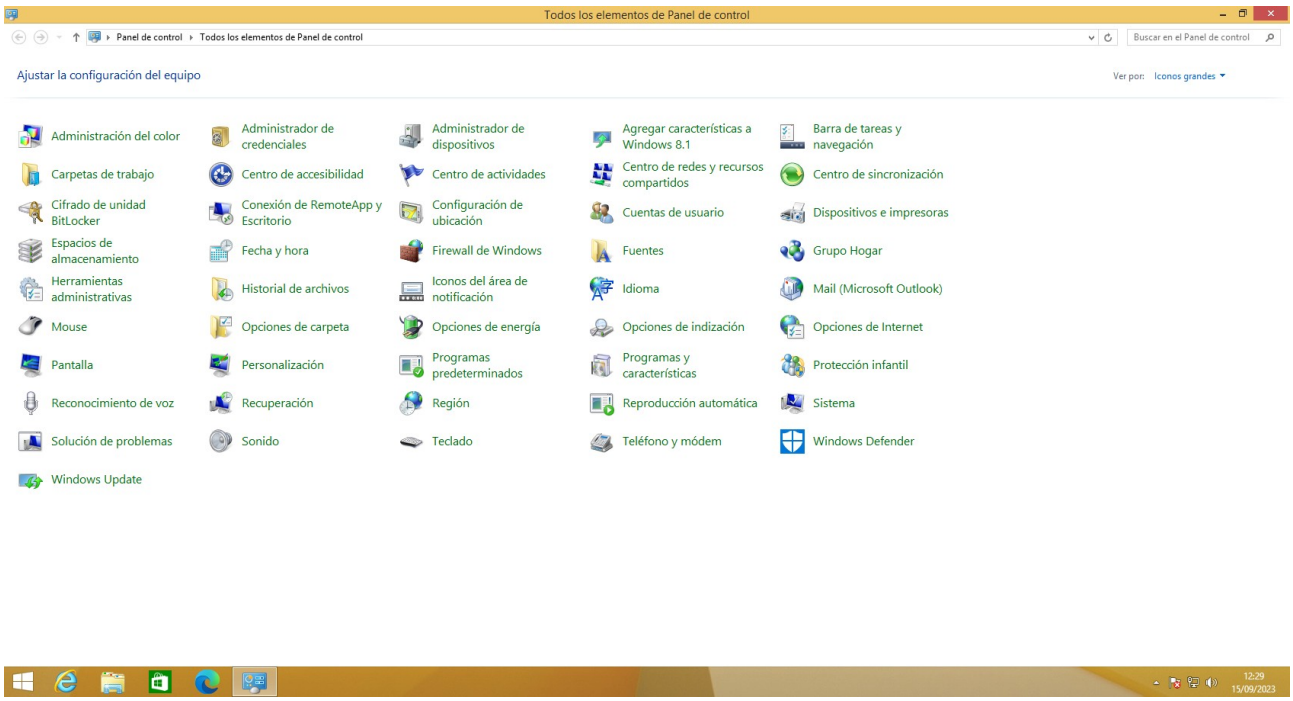
en dicho escritorio:



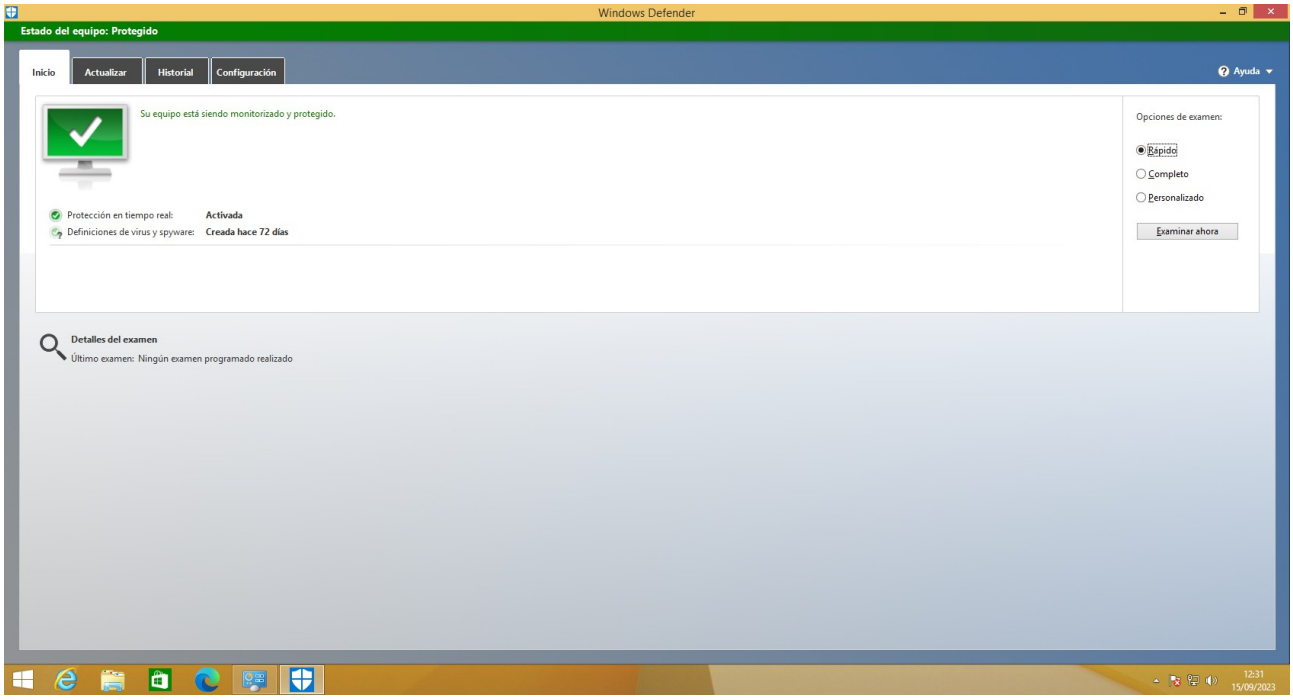
se va a inicio-flecha para abajo-panel de control:



ahora aquí:



nos iremos a “windows defender” y aquí:



si nos fijamos esta “rapido” (carpeta del sistema), “completo” (todo) y “personalizado” (selección del usuario)
- ¿Cómo se configura para tener el ordenador protegido?
Para configurar Microsoft Defender para una máxima protección puedes seguir estos pasos:
- Asegúrate de que las actualizaciones automáticas estén habilitadas para que Microsoft Defender esté siempre actualizado con las últimas definiciones de virus, en 8.1, estas actualizaciones se seleccionan manualmente en windows update, a partir de 10 se instalan solas.

- Activa la protección en tiempo real y la protección basada en la nube para obtener una detección y protección en tiempo real. En “seguridad de windows”:

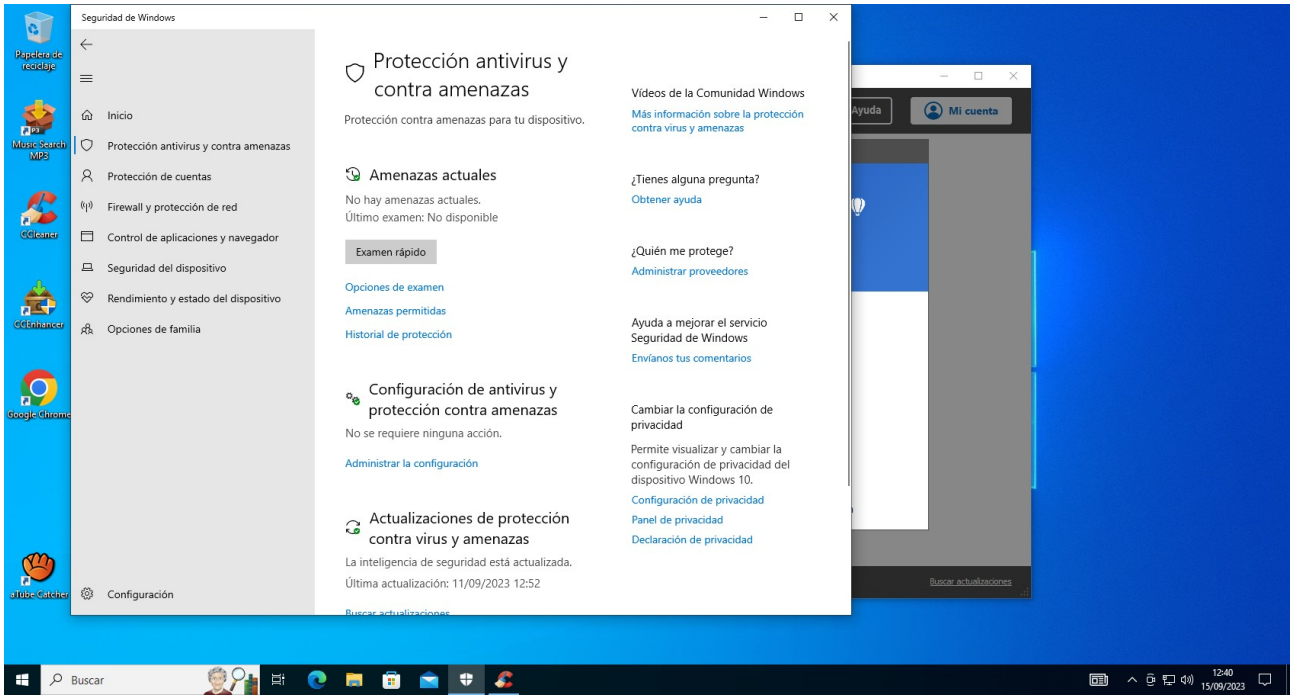
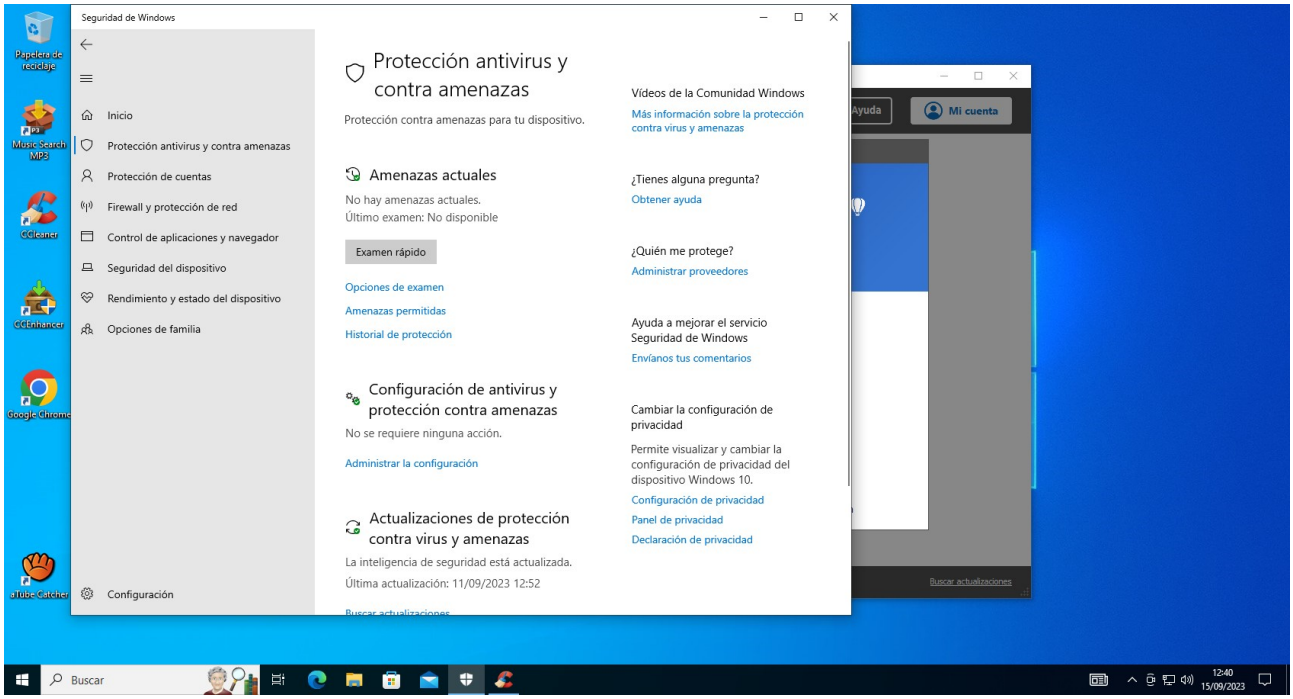
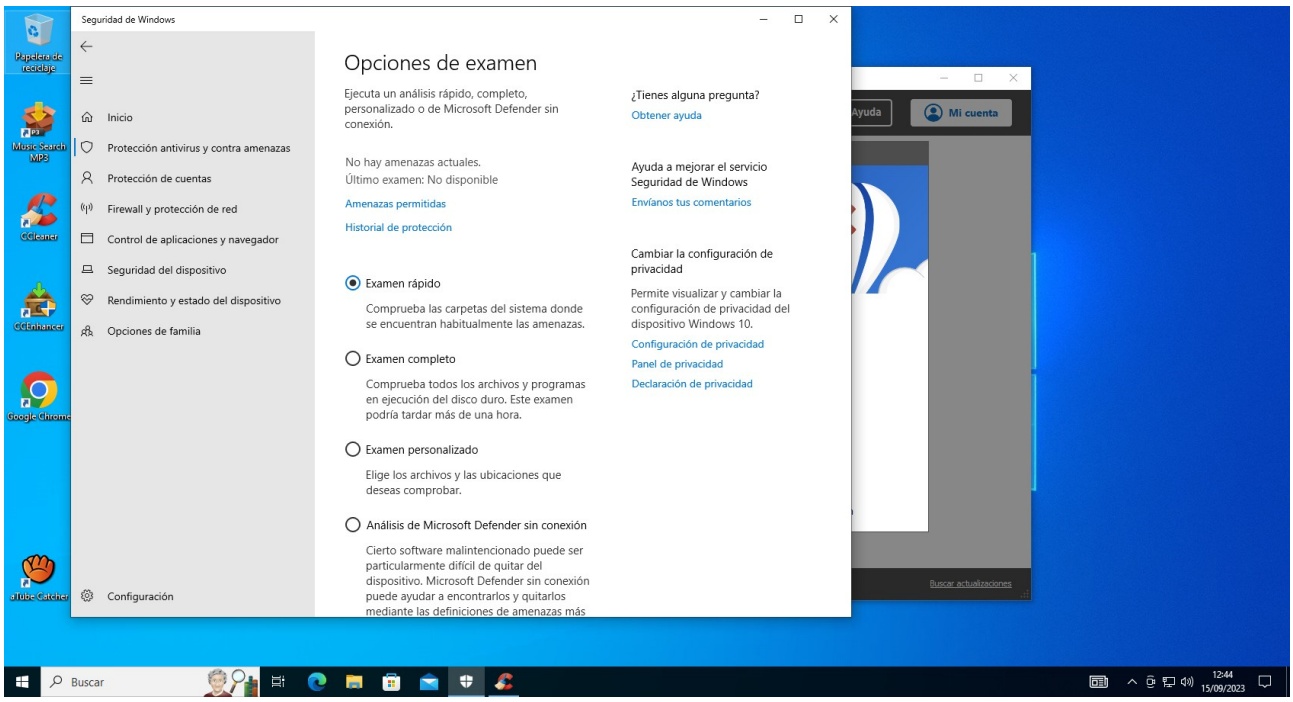


Figura 1: opcion de "proteccion contra antivirus y amenazas"

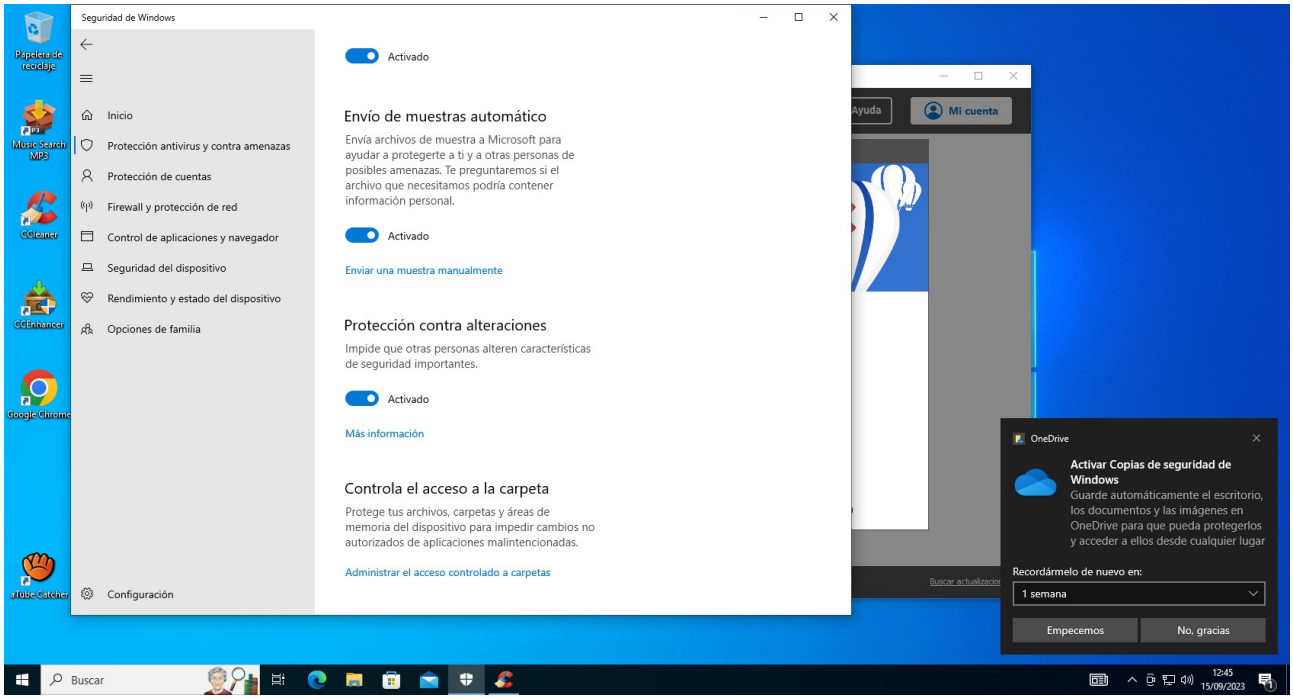
en la opcion de “configuracion de antivirus y proteccion contra amenazas”, le damos a “administrar la configuracion”, la opcion esta en la siguiente captura de pantalla:



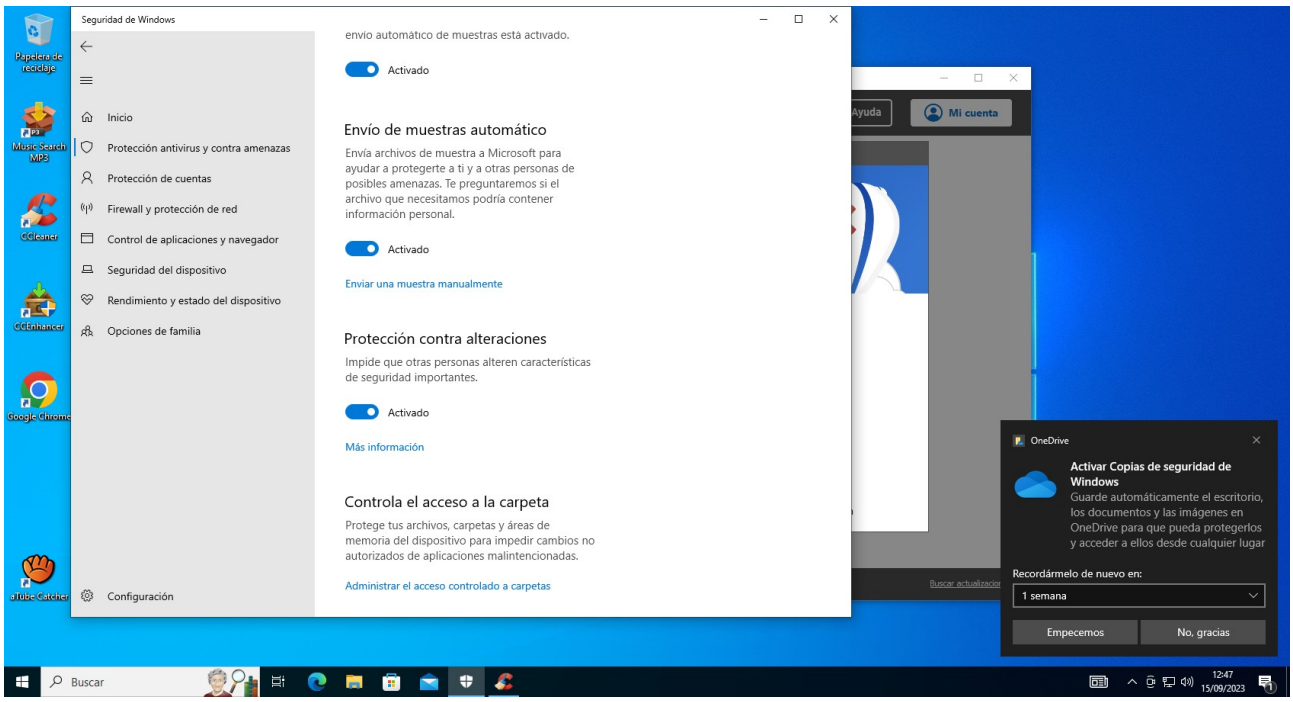
- Utiliza las opciones de examen rápido, personalizado, completo y sin conexión según sea necesario.



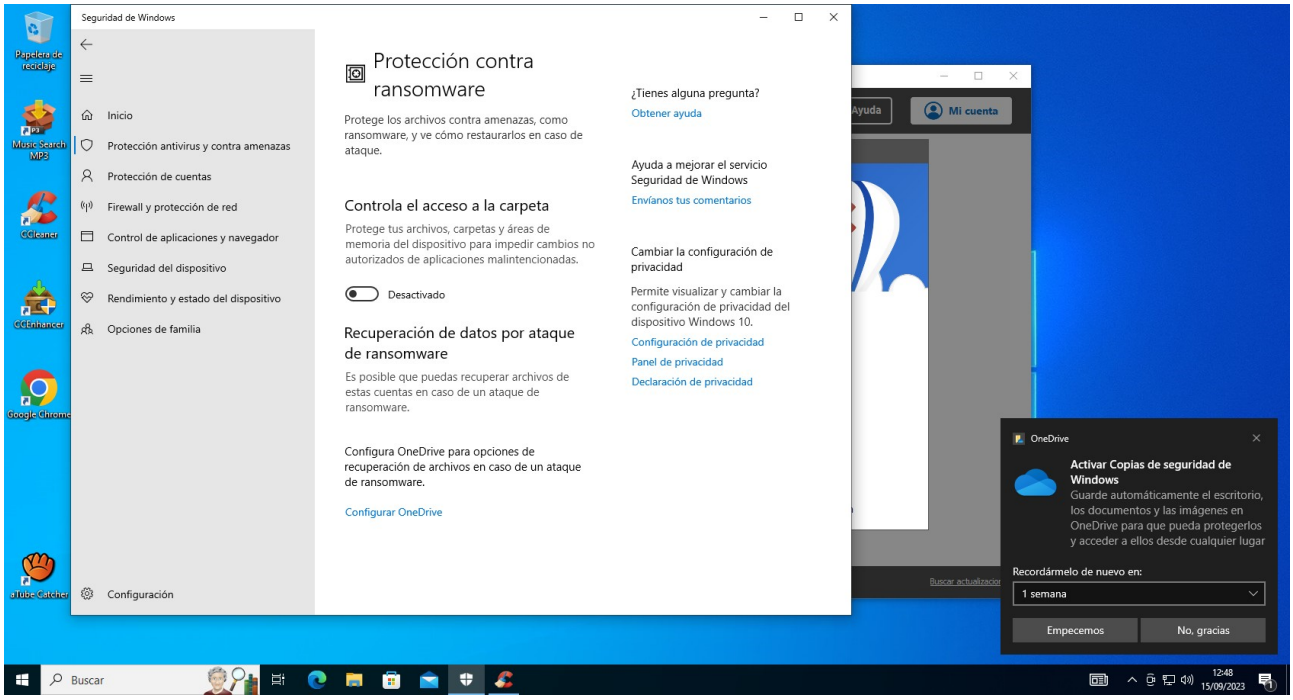
- Activa la protección contra alteraciones para evitar que los programas maliciosos desactiven las funciones antivirus, misma pantalla que la opcion de la proteccion en la nube:



- Utiliza el acceso controlado a carpetas para proteger tus archivos y carpetas importantes contra los cambios no autorizados por aplicaciones maliciosas, misma pantalla que la de arriba pero la opcion “controla el acceso a la carpeta”:



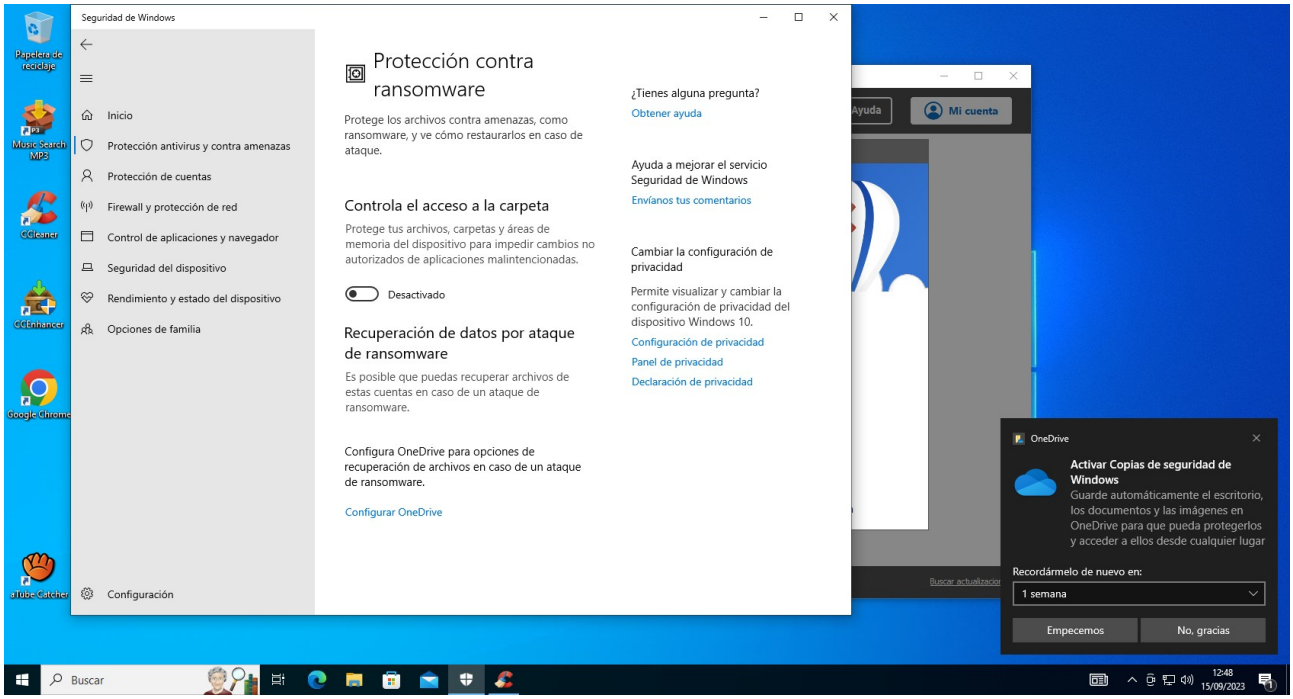
y esta seria la pantalla:



en donde si queremos, podremos proteger nuestros archivos de cambios realizados por programas malintencionados e incluso configurar onedrive para protegernos en caso de que nos secuestraran el ordenador (ransomware)

- En el caso de que quisiera desactivarlo, ¿cómo se desactivaría?
Para desactivar temporalmente la protección del Antivirus de Microsoft Defender en tiempo real en Seguridad de Windows puedes seguir estos pasos:
    - Selecciona Inicio y escribe "Seguridad de Windows" para buscar esa aplicación.
    - Selecciona la Seguridad de Windows de los resultados de la búsqueda, ve a Protección contra virus & amenazas.

- En Protección contra amenazas & virus, selecciona Administrar configuración.
- Cambia la Protección en tiempo real a Desactivado.



- Ventajas e inconvenientes de Windows Defender frente a otras soluciones de seguridad tanto de pago como gratuitas
Ventajas:
    - Es gratuito: No tiene ningún coste para el usuario.
    - Ya viene instalado: No hace falta descargar nada adicional.
    - Alto rendimiento: En la mayoría de las ocasiones el usuario no notará que lo tiene instalado.
    - Actualizaciones automáticas: Su base de datos es actualizada cada día.
Inconvenientes:
    - No es suficiente para usuarios avanzados: Si te mueves por páginas potencialmente peligrosas o utilizas programas P2P, Windows Defender puede quedarse corto frente a otros antivirus más robustos.
- No se puede desactivar rápidamente: A diferencia de otros antivirus, no se puede desactivar completamente con un solo clic. Se requiere seguir varios pasos para desactivarlo temporalmente.

Antivirus live

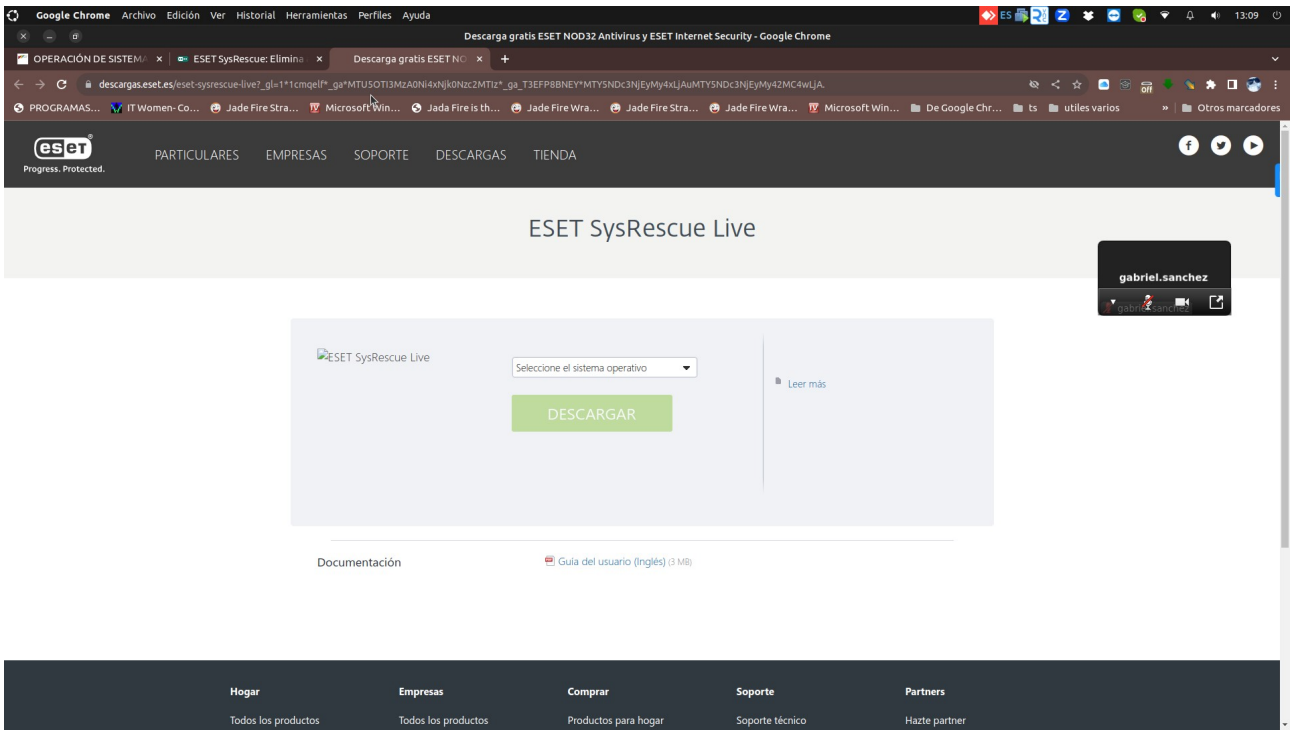
1. arranque del live CD de ESET:

primeramente, hay que conseguir otro equipo, logicamente, y ya desde otro equipo, seguir los siguientes pasos:

descargar la ISO:

https://www.eset.com/es/soporte/sysrescue/

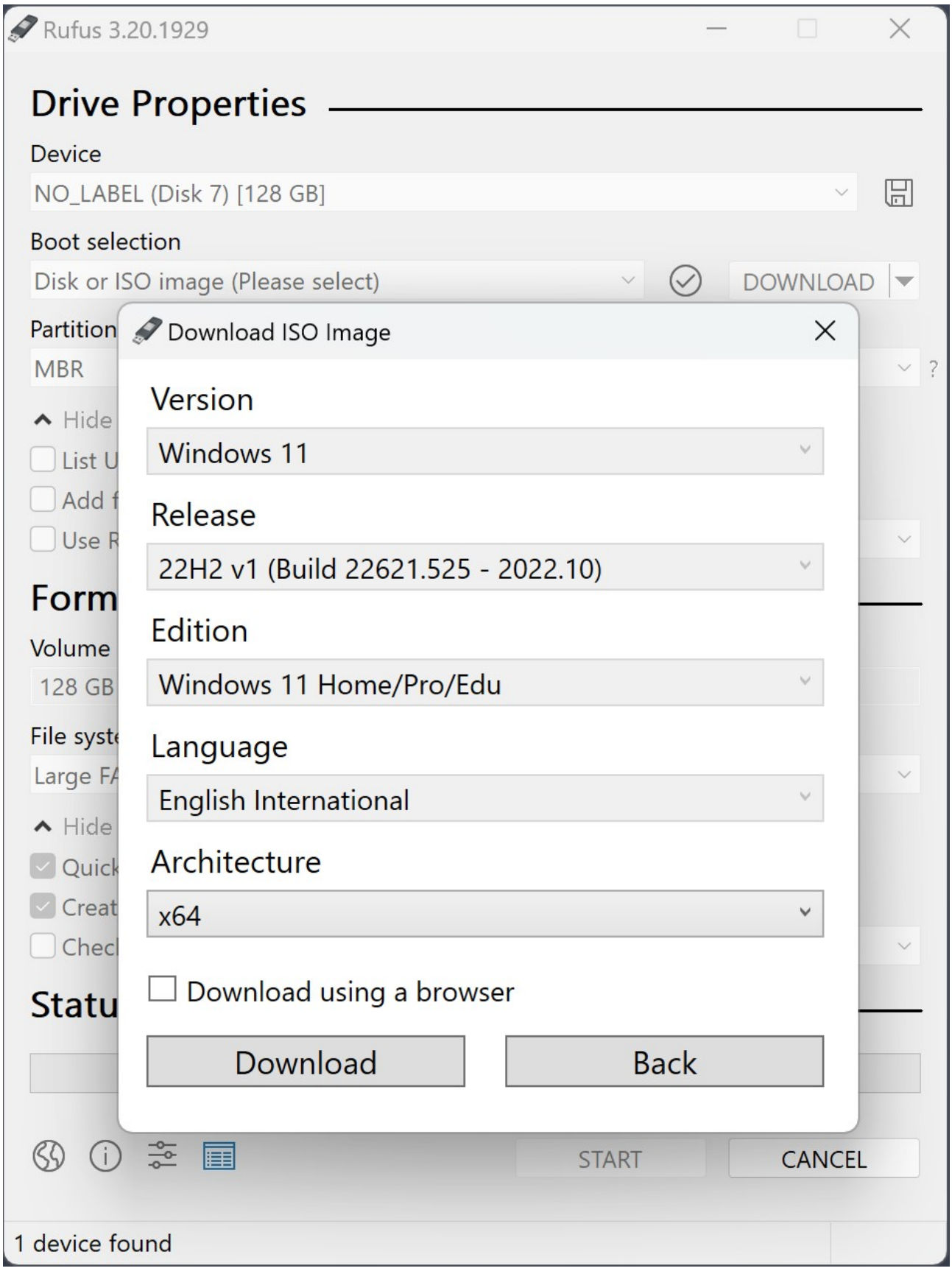
darle a “descarga gratuita” y atentos:



en “ESET sysrescue”, seleccionar “imagen ISO” si se quiere hacer el USB con Rufus o introducir la ISO con ventoy, si se esta en windows se puede usar la herramienta que nos suministra el ESET (solo compatible con windows).

La secuencia del rufus es:

seleccionar el pen
luego ir a select
seleccionar la ISO
darle a “empezar”
mensaje de “Esta seguro de que desea borrar” darle a OK



esperar a que finalice y ya estaria listo.

Sin embargo, si el sistema operativo es linux (si esta instalado en un equipo no compatible con 11 como core 2 duo o intel core I3-I5 e I7 antiguo que nos

hayan dado para hacer los medios para analizar el equipo infectado) hay varias maneras de proceder a hacer el tema, son las siguientes:

- usar ventoy (arrancar ventoy_x86.64 con sudo ./ en terminal) (recomendable para pendrives de 128 GB).
- usar balenaetcher, ir aquí:

https://github.com/balena-io/etcher/releases/

bajar el paquete deb y en terminal teclear:

sudo apt install ./INSTALADOR_ETCHER

otra forma es:

sudo dpkg -i INSTALADOR_ETCHER

si dice que hay paquetes a instalar, se instalan con:
sudo apt-get install -f

tercera forma, con gdebi (solo ubuntu, en debian hay que instalarlo manualmente):

sudo gdebi INSTALADOR_ETCHER

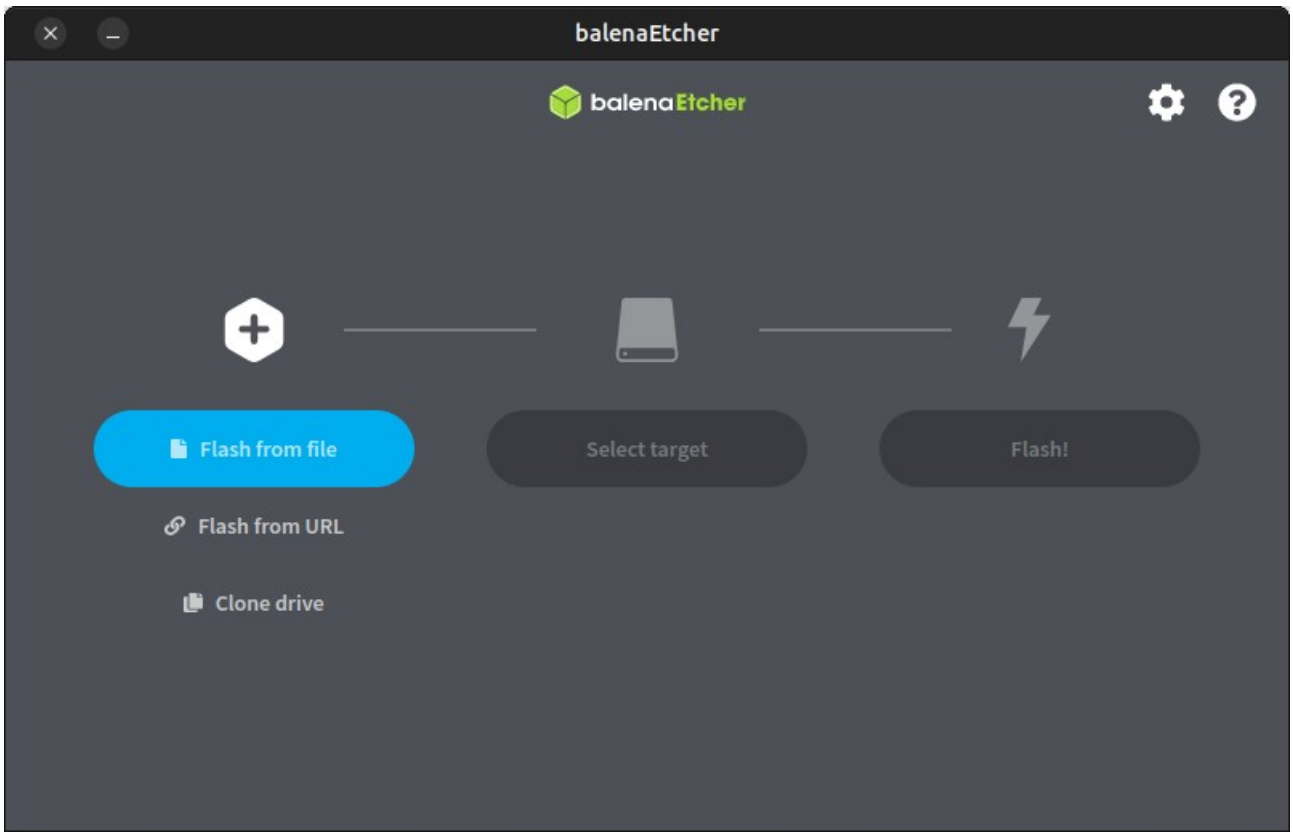
si es fedora, es este comando:

sudo yum localinstall INSTALADOR_ETCHER

y para opensuse:

sudo rpm -i INSTALADOR_ETCHER

luego en tema manejo es muy sencillo, aquí:



darle a “flash from file”, seleccionar la ISO linux, darle a “select target”, seleccionar el pendrive y darle a “flash”, el pendrive booteable con el live CD se realizara.

Esta solucion (que es una de las recomendaciones para poner en marcha las raspberry pi) esta disponible para windows y MACOS (arquitectura intel y apple), pero no se recomienda para hacer un booteable para windows, para instalar windows en por ejemplo un equipo que no sea compatible con virtualizacion, se deberan usar estas soluciones:

para windows:

herramienta de windows 10 y 11 (solo maquinas virtuales y equipos con arranque dual)
rufus
yumi (antigua BIOS y nueva BIOS)
ventoy

linux:

multibootusb (mejor forma de instalarlo, aquí: https://gitlab.com/cpcbegin/retromultiinstaller)
ventoy
woeUSB (desde la tienda de aplicaciones de python, se maneja por entorno comando unicamente), para instalarlo:

sudo apt-get update

sudo apt install git p7zip-full python3-pip python3-wxgtk4.0 grub2-common grub-pc-bin parted dosfstools ntfs-3g
sudo pip3 install WoeUSB-ng

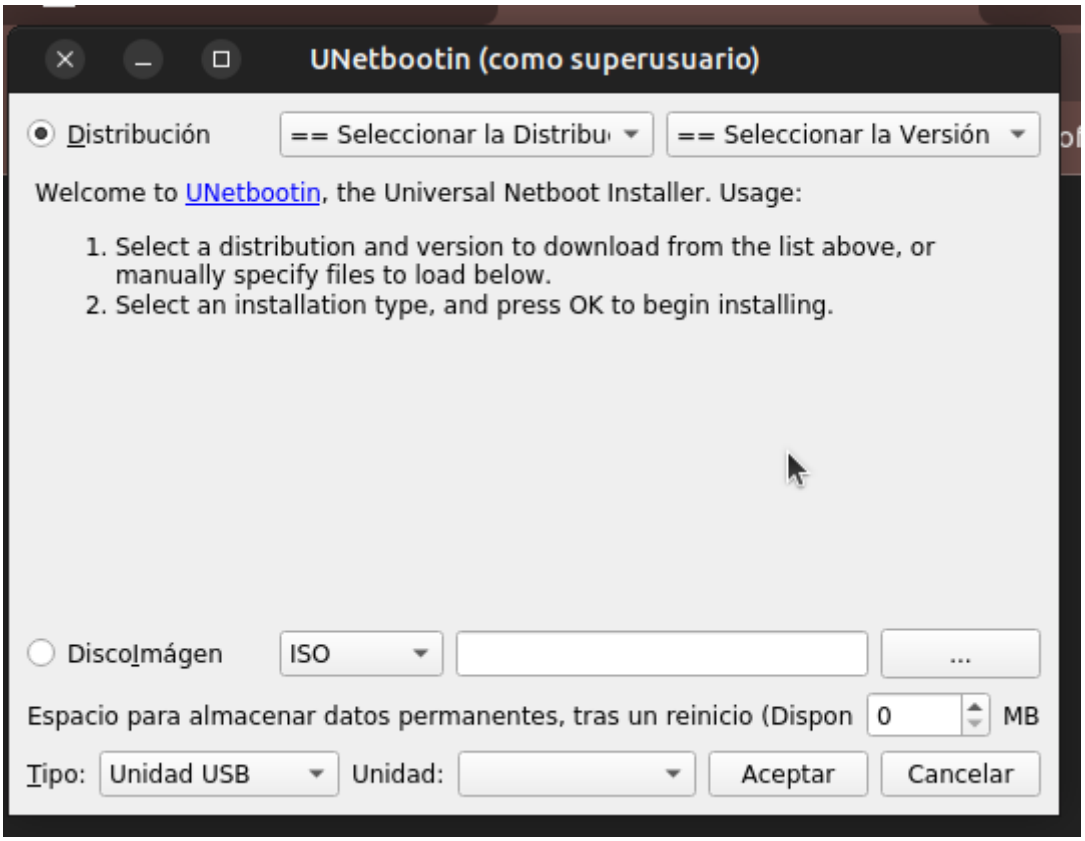
otra de las soluciones es unetbootin, descargar desde aquí:
http://unetbootin.github.io/linux_download.html
desde terminal, teclear:

sudo chmod +x EJECUTABLE_UNET

luego teclear este comando:

sudo ./EJECUTABLE_UNET

ahora aquí:



seleccionar “imagen”, luego boton de los tres puntos, seleccionamos la ISO, luego en “unidad USB”, selecciona el pendrive, darle a “aceptar” y se hara.

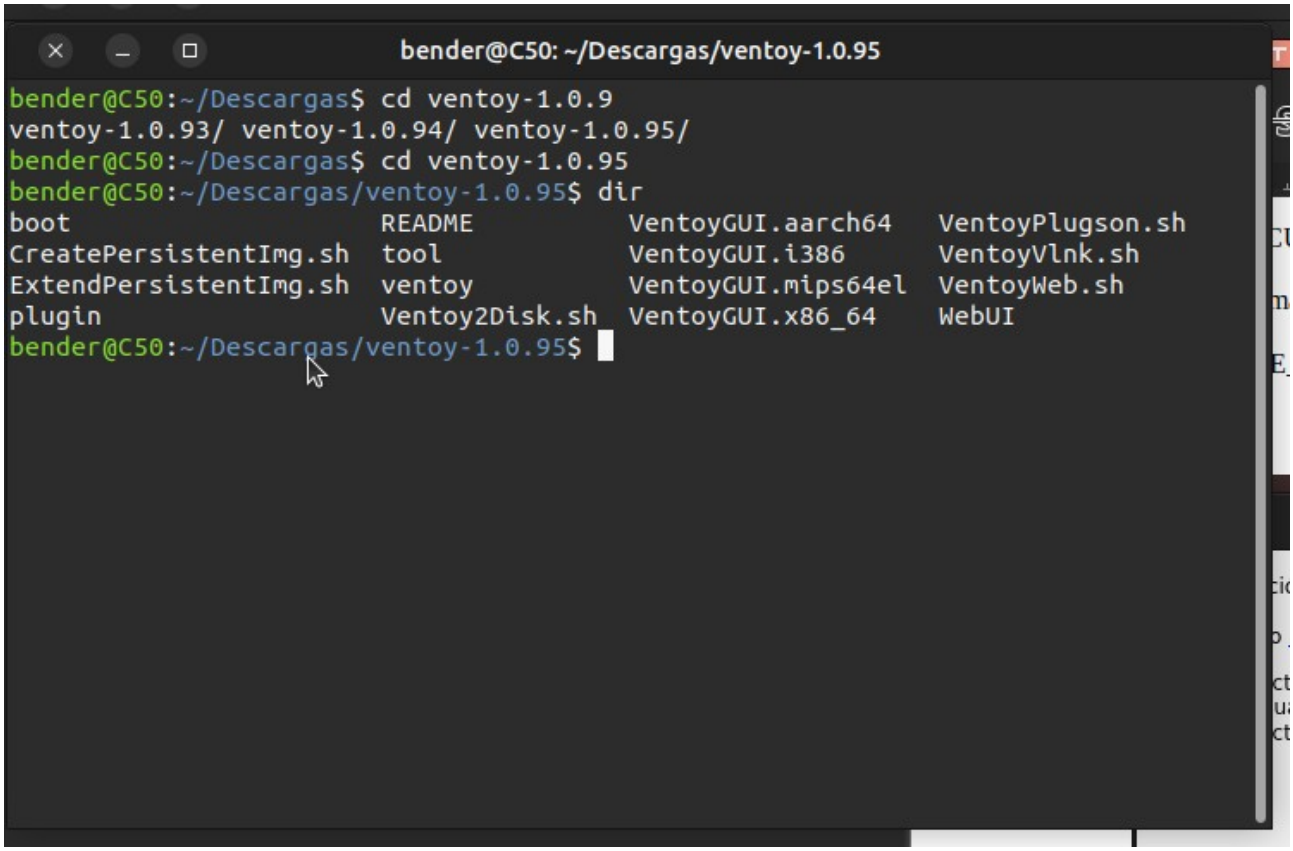
Con ventoy, se baja el ejecutable para windows o para linux:

https://github.com/ventoy/Ventoy/releases

en windows, doble clic, en linux, extraer el archivo (extraer aqui), boton derecho-abrir en un terminal, ir al directorio:

cd ventoy-1.0.9.5 (en mi caso esta version)

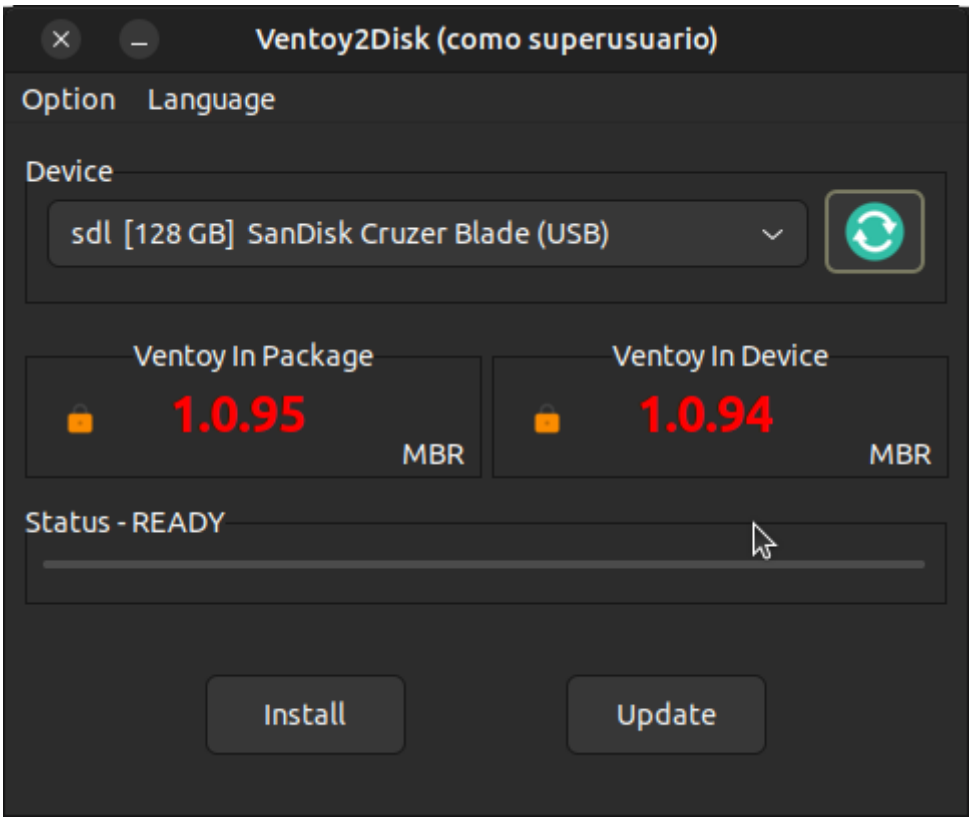
y aquí:



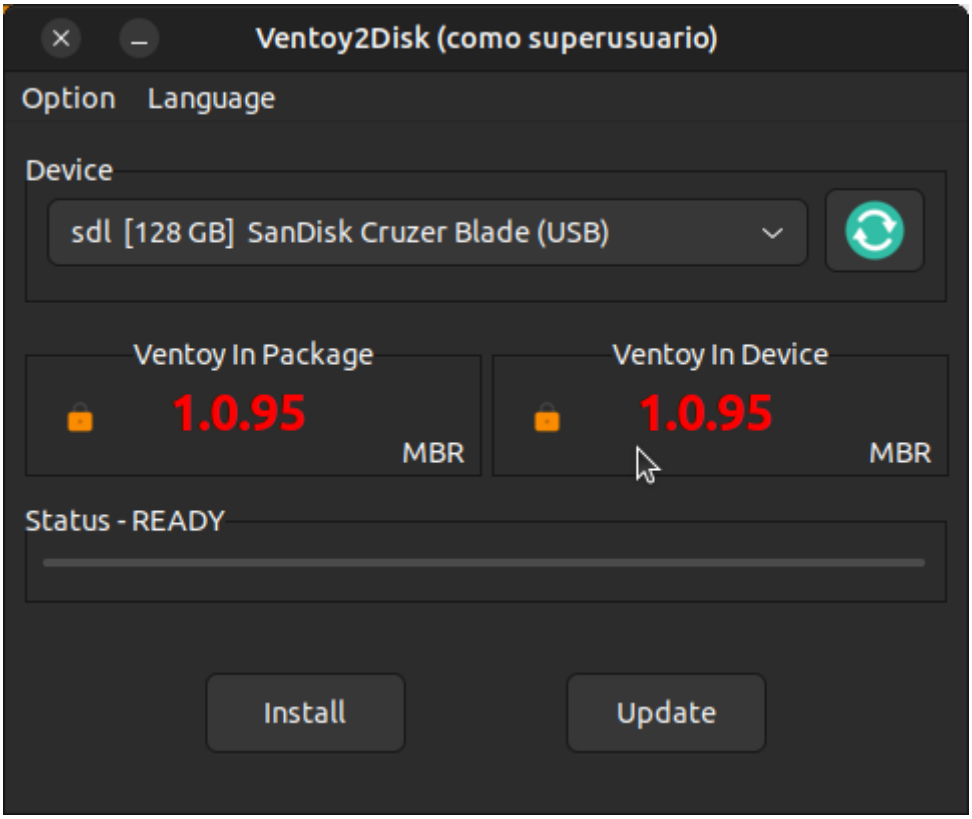
teclear:

sudo ./VentoyGUI.x86_64

teclear la contraseña y aquí:

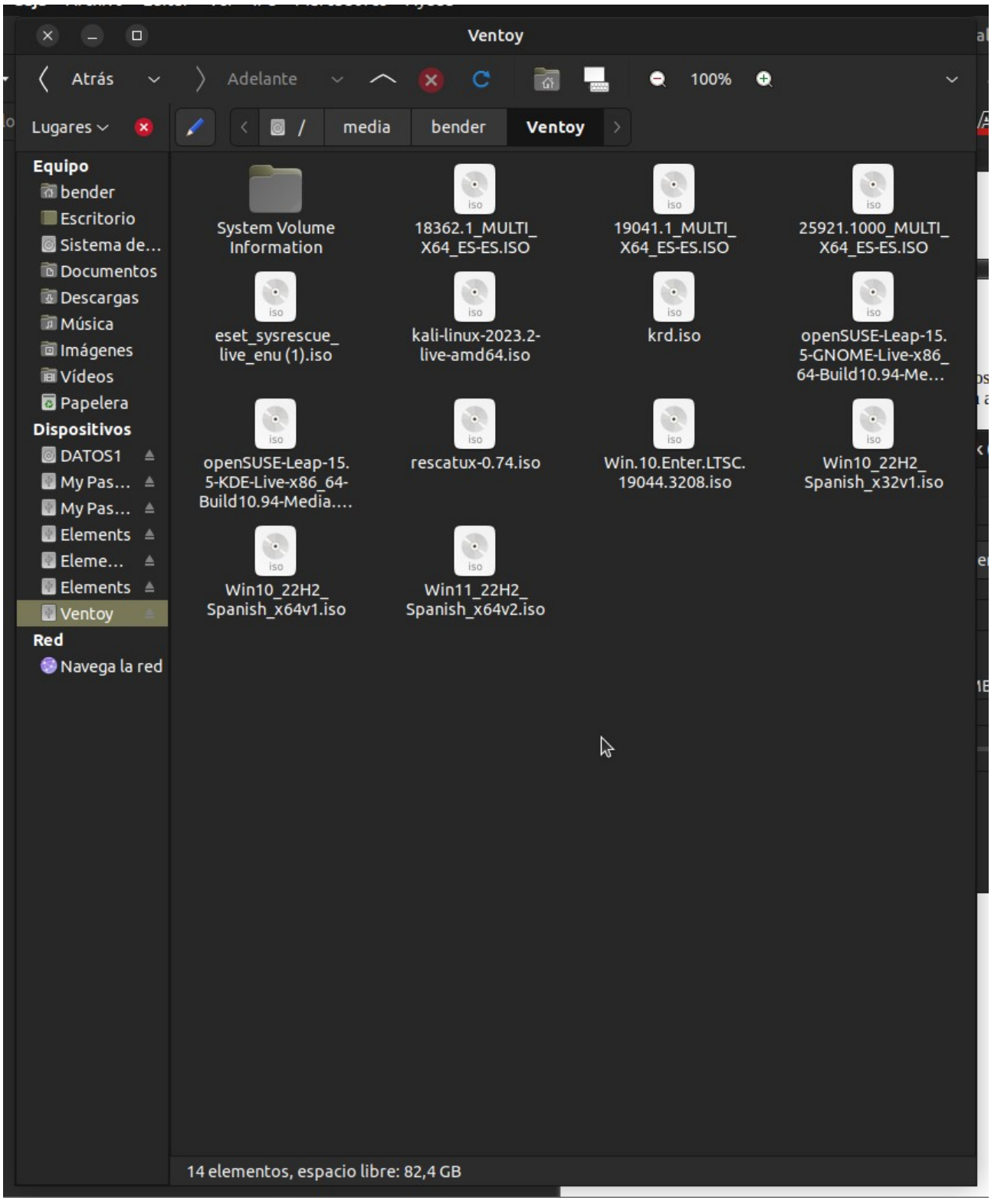


tanto windows como linux, si lo que queremos es crear el pendrive multiboot, dar a “install”, en mi caso, tengo una instalacion ya hecha, se le da a “update” para actualizarlo a la ultima version:



ya esta actualizado y listo para el multiboot.

Para colocar las ISOs es en esta unidad:



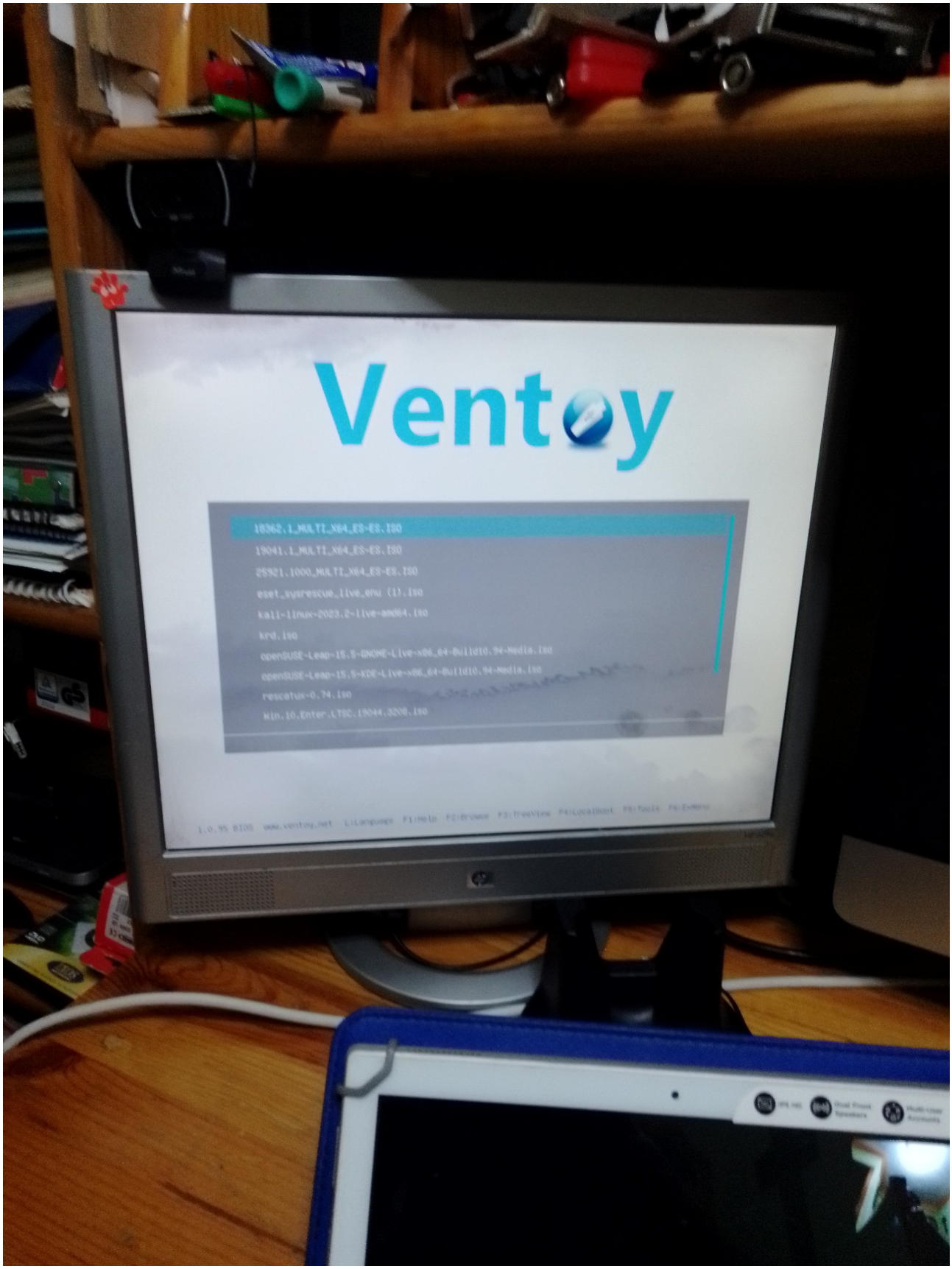
una vez ya colocada la ISO, boton de eject, esperamos a que desaparezca la unidad para que sea extraida, quitar el pendrive y ya estaria listo para bootear.

El metodo recomendado por kaspersky es el comando dd, la sintaxis seria:

dd if=ISO_ESET of=RUTA HACIA EL PENDRIVE[2] conv=fsync bs=4M

2 Sudo fdisk -l (averigua la ruta hacia la unidad) (se recomienda desconectar todas las unidades USB

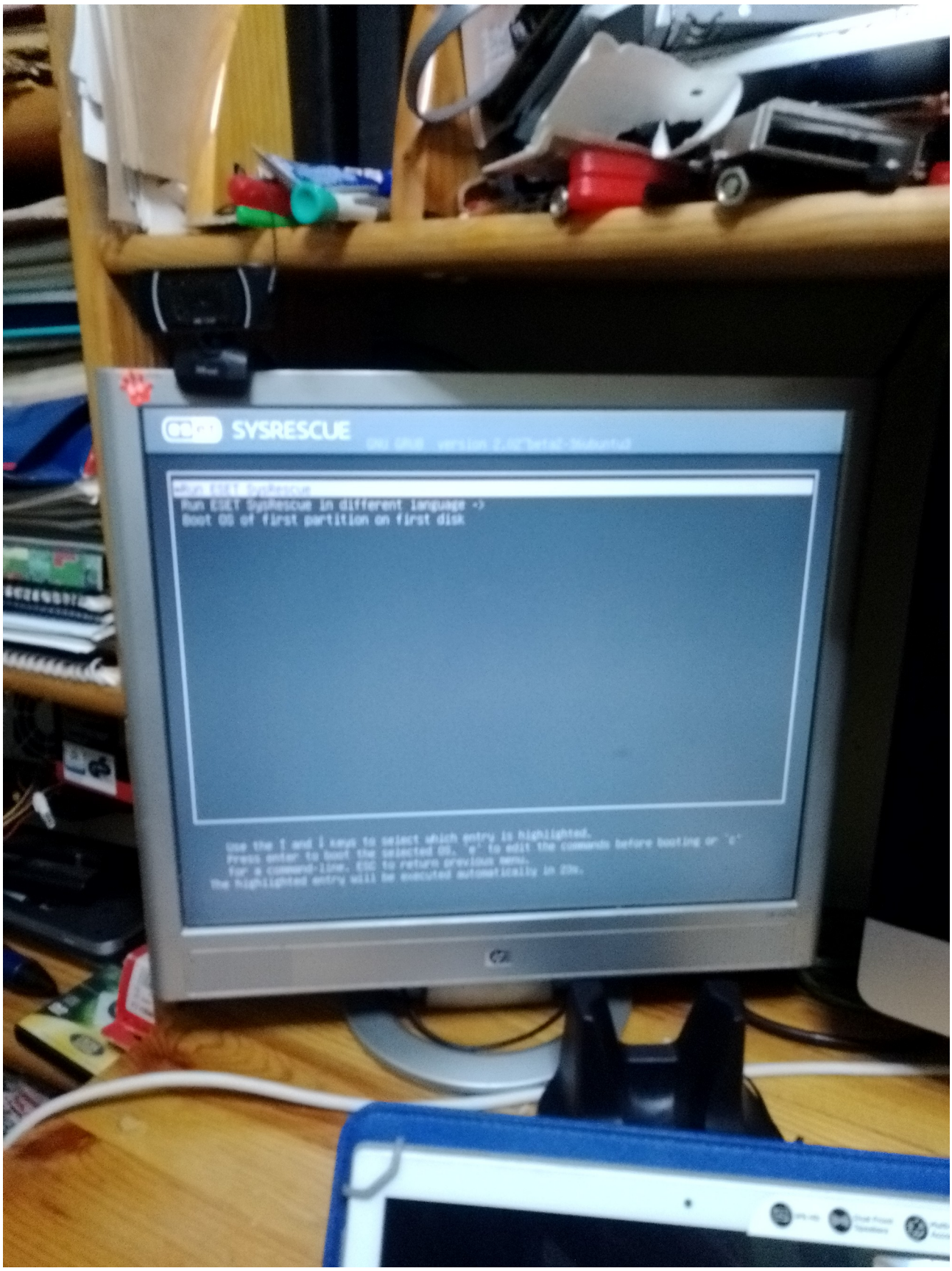
yo tengo las ISOs en ventoy, con lo cual se ha seleccionado ese, meter el pendrive, ahora darle a F12, seleccionar el pendrive y aquí:



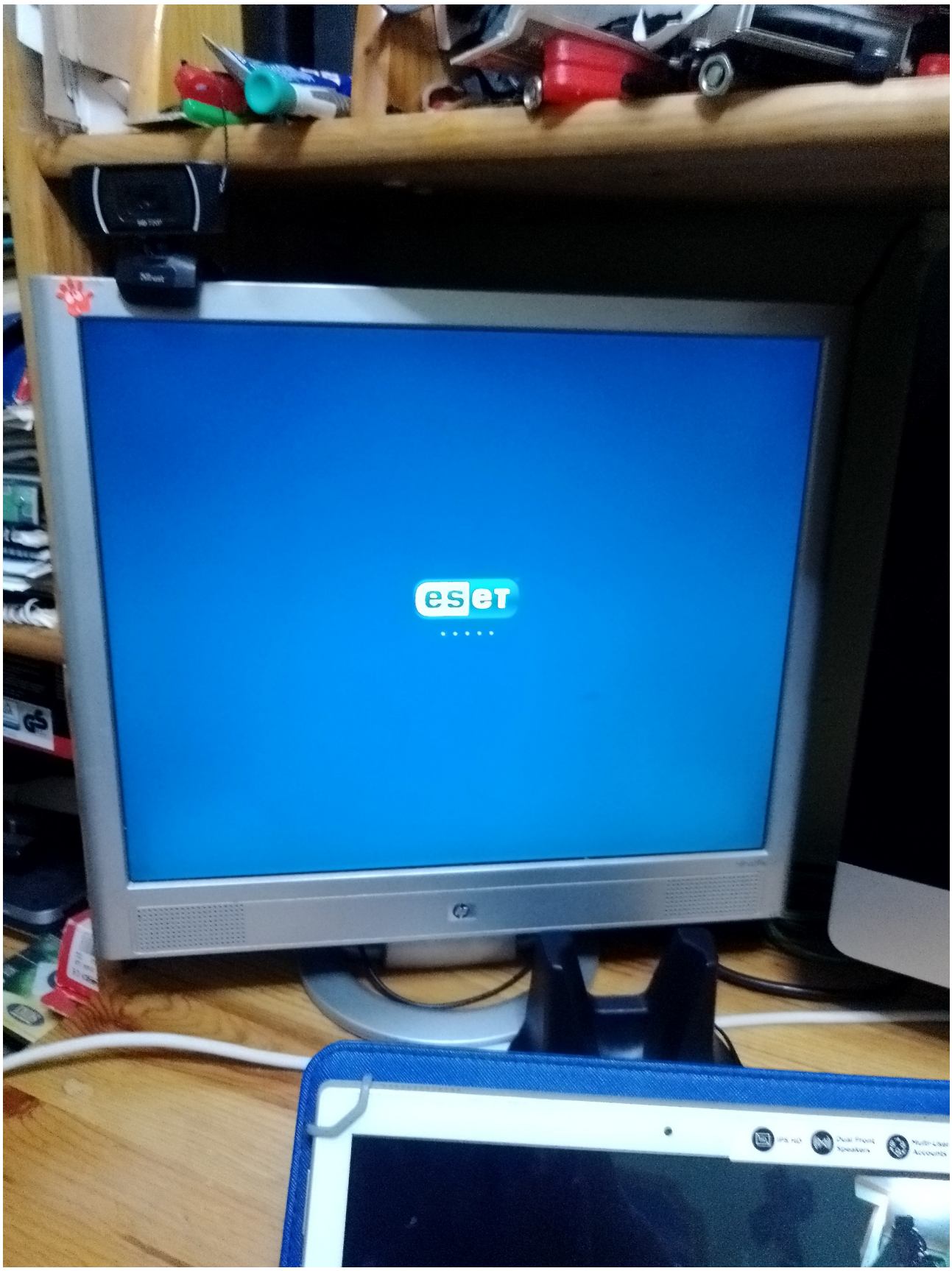
luego ir a la ISO del ESET y aquí:

seleccionar “normal mode”

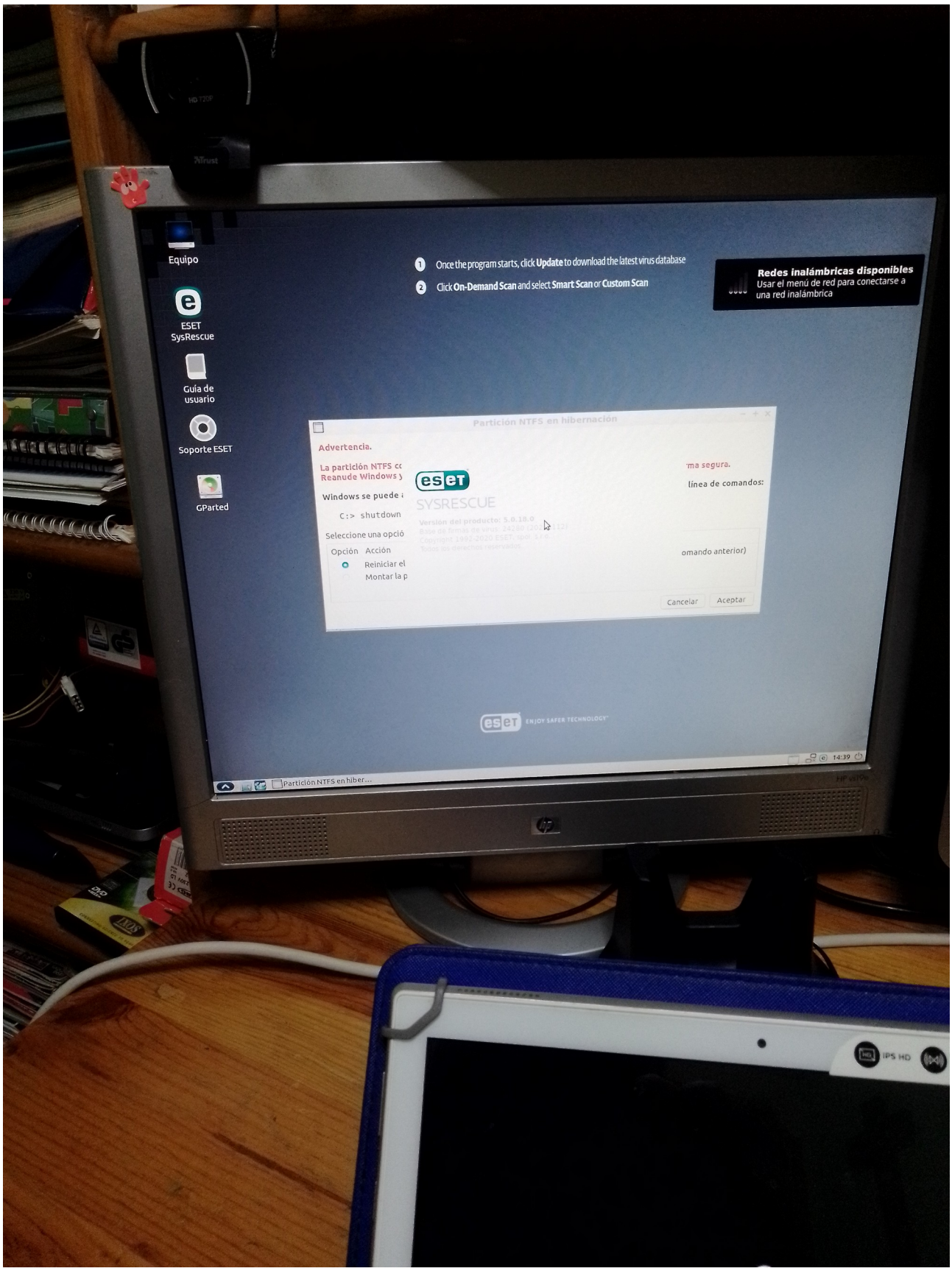
luego en la pantalla del live CD:



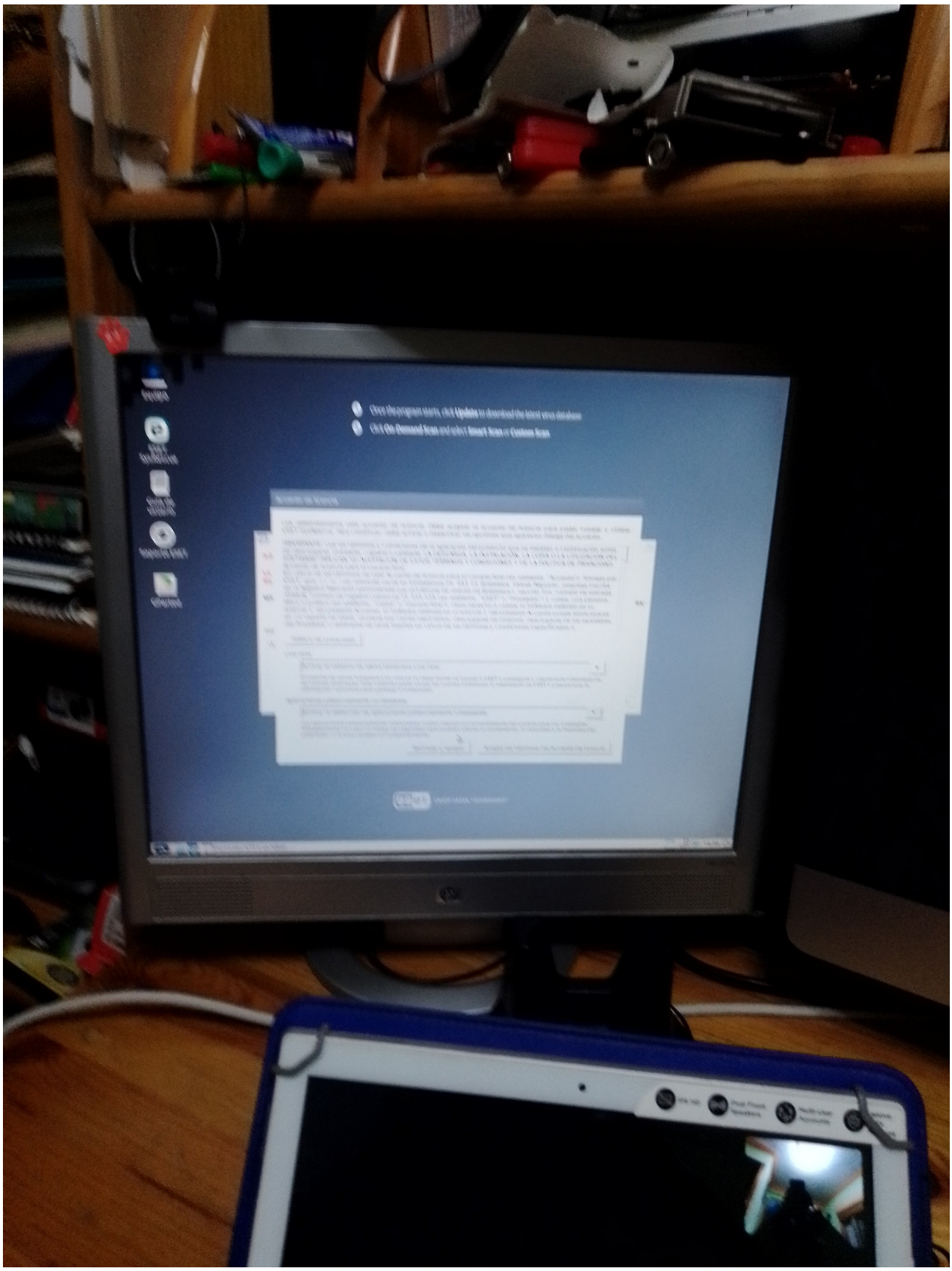
seleccionar “run ESET in different language”, seleccionar ES y se arrancara el live:



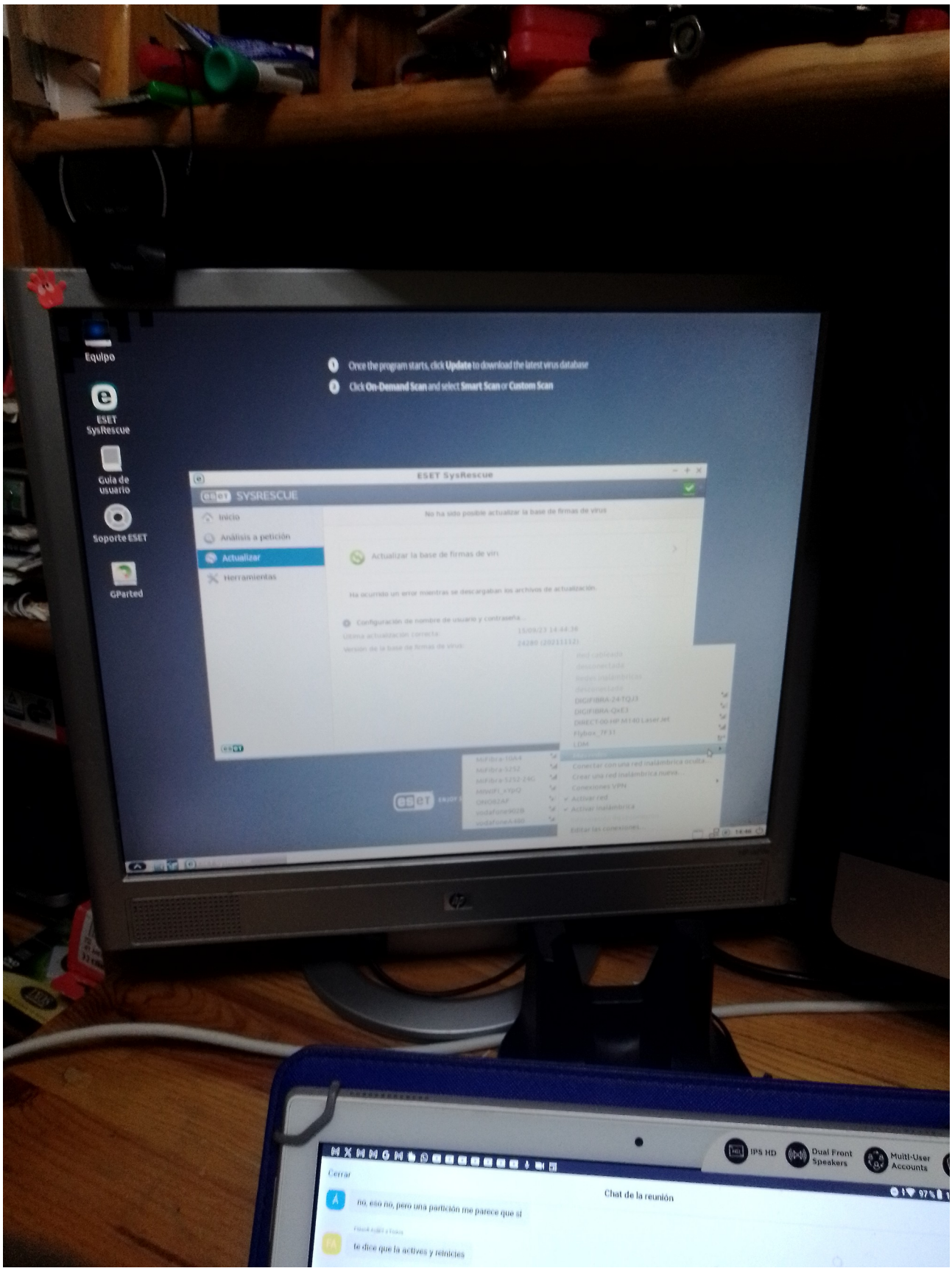
ahora aquí:


Equipo
ESET SysRescue
Guía de usuario
Soporte ESET
GParted
1 Once the program starts, click Update to download the latest virus database
2 Click On-Demand Scan and select Smart Scan or Custom Scan
Redes inalámbricas disponibles
Usar el menú de red para conectarse a una red inalámbrica
Partición NTFS en hibernación
Advertencia.
Windows se puede
C:> shutdown
Seleccione una opció
Opción Acción
Reiniciar el
Montar la p
línea de comandos:
omando anterior)
Cancelar
Aceptar
ESET
SYSRESCUE
ENJOY SAFER TECHNOLOGY
Partición NTFS en hiber...
14:39

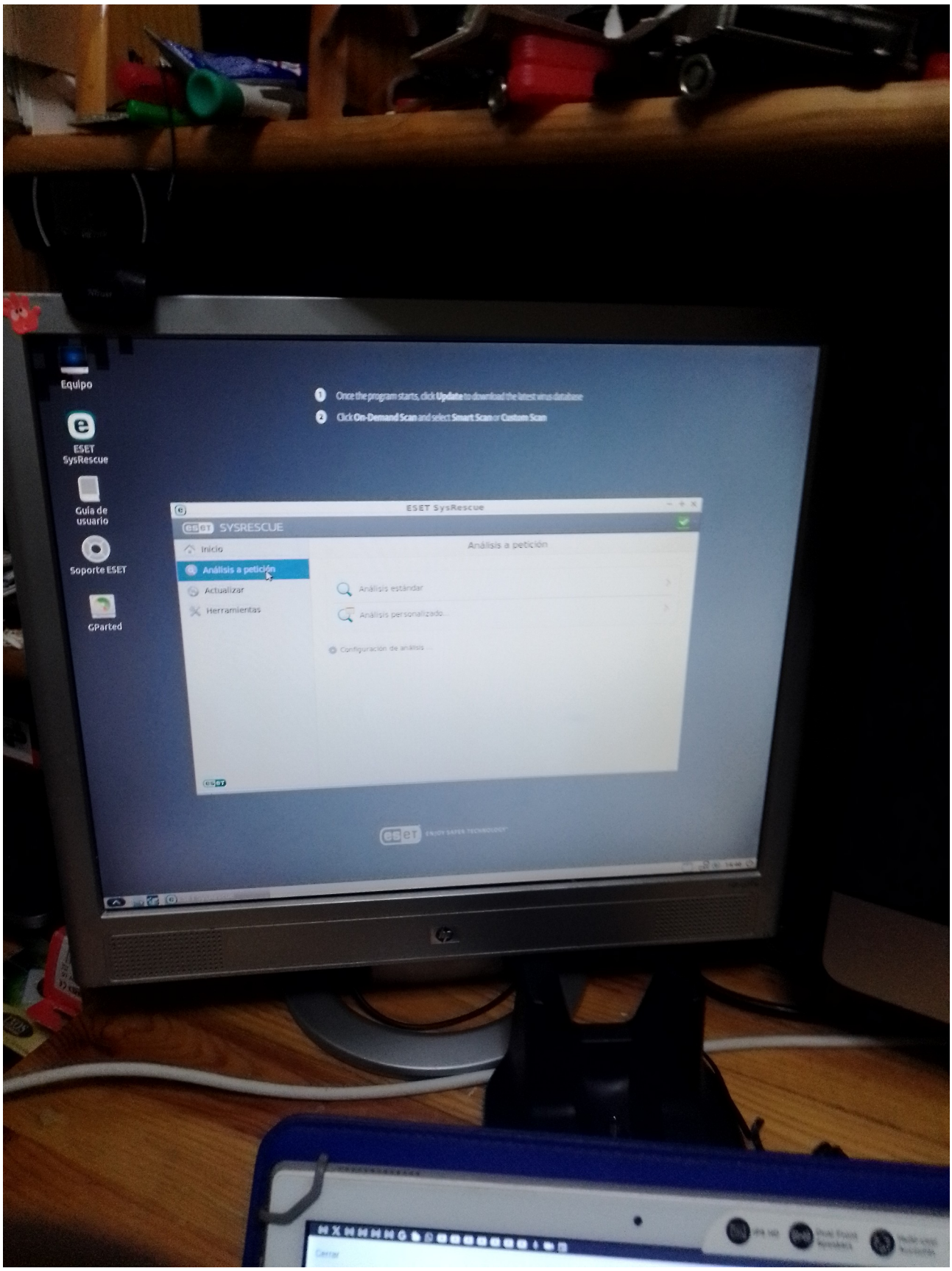
y ahora aquí:



las dos se seleccionan “ejecutar” y “iniciar”, luego en la pantalla del disco, todo a “aceptar”, bien, ahora seleccionar la WIFI y teclear la clave:



luego en “actualizar”, se actualizaran las firmas, ahora “analisis a peticion”, aquí:



“analisis estandar” y se iniciara el analisis, cuando finalice, boton azul-leave-reboot, se reiniciara el ordenador y ya estara analizado.